No. 24-1773

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT

REAL TIME MEDICAL SYSTEMS, INC.

Plaintiff-Appellee,

v.

POINTCLICKCARE TECHNOLOGIES, INC., d/b/a PointClickCare,

Defendant-Appellant.

On Appeal from the United States District Court for the District of Maryland, No. 8:24-cv-00313-PX, Hon. Paula Xinis

Appellant's Petition for Panel Rehearing or Rehearing *En Banc*

Rod J. Rosenstein
Amy R. Upshaw
Joshua N. Mitchell
KING & SPALDING LLP
1700 Pennsylvania Ave. NW
Washington, DC 20006
(202) 737-0500

Jeremy M. Bylund
Counsel of Record
WILLKIE FARR & GALLAGHER LLP
1875 K Street N.W.
Washington, DC 20006
(202) 303-1053
jbylund@willkie.com

William C. Jackson
GOODWIN PROCTER LLP
1900 N Street NW
Washington, DC 20036
(202) 346-4216

Counsel for PointClickCare Technologies Inc.

March 26, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Regulations

Rules

Other Authorities

RULE 40(b) STATEMENT

This case presents three questions of exceptional importance, each of which is a matter of first impression concerning a law that governs the exchange of all Americans' confidential electronic health records: (1) whether an actor engages in information blocking under the Cures Act where it offers electronic health information in two different means expressly identified by regulation; (2) whether a private party can sue for an alleged violation of the Cures Act; and (3) whether the defendant bears the burden of proof under the Cures Act to disprove a plaintiff's information-blocking claim.

INTRODUCTION

Rehearing is needed to correct fundamental errors committed by a panel of this Court—the first federal appellate court to review and interpret an electronic health information (EHI) custodian's obligations under the 21st Century Cures Act. Along with the Health Insurance Portability and Accountability Act (HIPAA), the Cures Act and its regulations govern the sharing of patients' EHI among EHI custodians and healthcare providers. The panel misapprehended federal laws and regulations in upholding an injunction ordering a private EHI custodian to abandon its security protocols and give automated software "bots"

unfettered access to its system and patient EHI. If allowed to stand, the panel's opinion will require EHI custodians to bear the burden in costly litigation to enforce routine security protocols that protect Americans' sensitive EHI.

Plaintiff Real Time Medical Systems (RTMS) obtained a preliminary injunction preventing defendant PointClickCare from enforcing its contractual ban and security protocol barring bots. Barring third-party bots is an ordinary security feature of many online platforms. Without such a bar, bots can run high volumes of queries, which cause access slowdowns and system unavailability and pose security risks. The district court held that, based on the record before it, the Cures Act required PointClickCare to provide RTMS's bots access to its system. A panel of this Court affirmed in a published opinion. — F.4th —, 2025 WL 779691 (Mar. 12, 2025); *see generally* COA.R.52 ("Op."). In counsel's judgment,[1] the panel overlooked several significant legal matters on a question of exceptional importance to the healthcare sector, which is responsible for protecting sensitive health data.

[1] *See* 4th Cir. R. 40(b).

First, the panel misapprehended the regulatory "manner exception" to the information-blocking prohibition. This exception allows a custodian to provide EHI through standard means where the requestor and custodian are unable to reach agreement for nonstandard access. 45 C.F.R. § 171.301. Without any justification in the text, the panel interpreted this provision to bar an EHI custodian from providing standardized terms and instead required all custodians to undertake time- and cost-intensive negotiations. The panel further held that PointClickCare's offer of alternatives the regulation requires did not suffice.

Second, the panel misapprehended Maryland and federal law by allowing a private party to sue for a Cures Act violation. The Cures Act does not create a private cause of action. Instead, the Cures Act has a reticulated enforcement scheme that allows for significant governmental discretion. RTMS circumvented that limitation by nesting a Cures Act violation in a state unfair-competition claim. But to determine whether a regulatory violation can give rise to an unfair-competition claim, Maryland law looks to whether such a claim is consistent with the federal scheme. Here, it is not.

Third, the panel inverted the burden of proof on Cures Act claims. The Cures Act describes information blocking in broad terms as anything likely to interfere or discourage the exchange of electronic health information. 42 U.S.C. § 300jj-52(a)(1). It then directs the agency to identify "necessary activities that do not constitute information blocking." *Id.* § 300jj-52(a)(3). These necessary activities, though styled as "exceptions," are essential elements of the claim. *See United States v. Cook*, 84 U.S. (17 Wall.) 168, 173-74 (1872). The plaintiff accordingly has the burden of proof to establish that the defendant's conduct fell outside the regulatory exceptions. The panel, however, held that the defendant carried the burden to disprove plaintiff's claim. In doing so, the panel opened the floodgates to litigation. All companies that store EHI now face the prospect of being haled into court and subject to sensitive discovery if they decline to give requestors access to patients' private data using any means the requestor demands. Such a regime conflicts with the cooperative and interoperative scheme Congress created.

BACKGROUND

Statutory and regulatory background. The Cures Act and its implementing regulations seek to increase interoperability of EHI while

maintaining that information's privacy and security. Op.8-9. The Cures Act bars "information blocking"—any activity that "is likely to interfere with, prevent, or materially discourage access, exchange, or use" of EHI. 42 U.S.C. § 300jj-52(a)(1)(A). But it directs HHS to "identify reasonable and necessary activities that do not constitute information blocking." *Id.* § 300jj-52(a)(3).

In notice-and-comment rulemaking, HHS identified ten such reasonable and necessary activities. Under one of them—the "manner exception"—a custodian need not grant access in a nonstandard format. Requestors are free to negotiate for nonstandard access, but the manner exception provides that if the parties cannot agree on terms, the EHI custodian may instead provide data in standardized manners outlined in the regulations. 45 C.F.R. § 171.301.

The Cures Act vests enforcement exclusively in the federal government, giving HHS's Office of the Inspector General (OIG) authority to investigate information blocking. 42 U.S.C. § 300jj-52(b)(1). If OIG finds that an entity engaged in information blocking, it may impose penalties. *Id.* § 300jj-52(b)(2).

Factual background. PointClickCare provides EHI storage and access for thousands of skilled nursing facilities across North America. Like most data custodians, PointClickCare's contracts prohibit the use of automated software bots because they pose security risks and strain system resources. PointClickCare uses security protocols to prevent accounts associated with bot usage from accessing its system.

RTMS analyzes patients' health data and provides automated recommendations to the patients' healthcare providers. RTMS does not contract with PointClickCare but with individual facilities; it accesses PointClickCare's system through login credentials those facilities provide. RTMS then downloads patient data using disruptive, high-speed bot queries. JA640, JA845. As RTMS's business has expanded, those bots have caused cascading access problems for PointClickCare's customers, putting their patients' lives at risk. When PointClickCare began to address those outages by employing security methods that prevented bots—including those RTMS controls—from operating on PointClickCare's system, RTMS sued and obtained a preliminary injunction, based on a state unfair-competition claim incorporating an

alleged violation of the Cures Act, that requires PointClickCare to allow RTMS to use bots on its system. The panel upheld that injunction.

ARGUMENT

I. The panel misapprehended the manner exception and overlooked key regulatory text.

The manner exception allows an EHI custodian to limit the manner in which it fulfills a request for EHI without engaging in "information blocking." 45 C.F.R. § 171.301. The custodian need not provide EHI access in the manner requested where it "cannot reach agreeable terms with the requestor." *Id.* § 171.301(a)(1). In that circumstance, the custodian may meet its Cures Act obligations by offering standardized access methods. *Id.* § 171.301(b). Once it has offered two alternatives, it has met its obligations under the Cures Act. *Id.* § 171.204(a)(4)(ii). Here, the parties could not reach agreeable terms because PointClickCare contractually *bars all bots* from accessing patient data on its system. So PointClickCare offered RTMS two standardized alternative methods of access.

The panel misunderstood both prongs. Relying on language from HHS rulemakings, the panel grafted onto the manner exception an atextual requirement that PointClickCare present evidence of "genuine

efforts" to reach agreement with RTMS on nonstandard access requests. Op.47. And the panel further faulted PointClickCare for the alternatives it made available to RTMS. Op.40.

A. The panel's individualized-negotiation rule conflicts with the manner exception's text and HHS's interpretation.

The manner exception allows an actor to supply electronic health information through standardized means when "the actor … cannot reach agreeable terms with the requestor" for nonstandard access. 45 C.F.R. § 171.301(a). That provision means what it says: parties may use nonstandard means to share information when *both parties agree* to the terms. Here, it is undisputed that the parties did not find "agreeable terms" for RTMS's requested bot usage.

The panel, however, added an additional requirement that an EHI custodian present evidence of "genuine efforts" to reach agreement with a requester. Op.47. According to the panel, an actor cannot offer a slate of standardized terms but must undertake time-intensive, one-off negotiations for every non-standard request. To justify its ruling, the panel lifted select language from the manner exception's rulemaking. Op.43-47 (citing 85 Fed. Reg. 25,642, 25,649, 25,877 (May 1, 2020)). But

the panel failed to follow "the first rule of … interpretation," which is "Read on." *Bledsoe v. Cook*, 70 F.4th 746, 749 (4th Cir. 2023).

HHS considered this very issue and reached the opposite conclusion. In its rulemaking, HHS explained that one of the Manner Exception's central goals was to "offer[] certainty that an actor's practices that fully satisfy the Manner Exception's conditions will not be considered information blocking" and to "incentivize offering an alternative manner (*with priority to interoperable manners based on HHS-adopted and available open standards*)." 89 Fed. Reg. 1192, 1381 (Jan. 9, 2024) (emphasis added). By doing so, HHS sought to alleviate the "problematic level of uncertainty about whether [actors] will be engaging in information blocking if they decline demands from requestors for non-standard … solutions that they do not currently support *even after* they have offered to provide access, exchange, or use of EHI in the same manner(s) the actor makes generally available to its customers or affiliates, *and* through standards-based manners, consistent with § 171.301." *Id.*

The panel's view that PointClickCare was required to negotiate a tailor-made solution for RTMS misapprehends the regulation. HHS did

not want EHI custodians to "divert their development capacity to fulfilling requested manners of access" for requestors who "are *unwilling* … to agree to terms … for their requested manner *or* any alternative manner consistent with the Manner Exception." *Id.* (emphasis added). Instead, HHS crafted the Manner Exception to allow requestors to receive nonstandard access only when they agree to the actor's terms. Otherwise, the actor can satisfy its obligations by providing information through the alternatives outlined in the regulation. The panel misapprehended the regulation's text and purpose. Rehearing is warranted.

B. The panel's determination that providing standardized (USCDI) data is an inadequate alternative conflicts with the regulation.

The panel also overlooked the regulatory text when it concluded that providing United States Core Data for Interoperability (USCDI) data was insufficient to satisfy one of the alternative-manner prongs under the manner exception. Where the parties cannot reach agreeable terms, an actor satisfies its information-blocking obligation by offering "at least two alternative manners." 45 C.F.R. § 171.204(a)(4)(ii). These alternatives include (1) using technology certified to standards adopted

in part 170 and (2) using "content and transport standards" published by the federal government. 45 C.F.R. § 171.301(b). It is undisputed that PointClickCare offered RTMS access to all of the data it requested through its human access to PointClickCare's EHI platform—a Part 170-certified system. Reply Br. 12; *see* 45 C.F.R. § 171.301(b)(1)(i). The panel's conclusion that PointClickCare did not offer a means of access for all the data RTMS requested is simply wrong. In addition, PointClickCare offered RTMS access to USCDI data, which is a content and transport standard published by the federal government. *See* JA289-290 ¶ 9.

The panel overlooked the plain text of the regulation and held that offering USCDI data was not an adequate alternative. *See* Op.40-42, 44-45. The panel mistakenly explained that "[t]oday's manner exception refers to the *manner* of delivery, not the *content* to be delivered." Op.40. To the contrary, the manner exception expressly allows an actor to fulfill a request "[u]sing *content* and transport standards" published by the

federal government." 45 C.F.R. § 171.301(b)(1)(ii) (emphasis added); *see also* 45 C.F.R. § 171.204(a)(4).[2]

The panel's confusion appeared to stem from the manner exception's regulatory history. Before 2022, an EHI custodian could satisfy the manner exception even if it provided only "the electronic health information identified by the data elements represented in the USCDI standard." *See* 45 C.F.R. § 171.301(a)(1) (2020). That content condition was removed from the text of the manner exception. *See* 89 Fed. Reg. at 1372.

But the manner exception continues to authorize USCDI data as one of the required alternatives because it is a "content and transport standard[] published by … [t]he Federal Government." 45 C.F.R. § 171.301(b)(1)(ii). Indeed, the very same rulemaking that converted the former "Content and Manner Exception" to the "Manner Exception," *see*

[2] Although the text of the manner exception refers to alternative manners "specified by the requestor," 45 C.F.R. § 171.301(b), the "manner exception exhausted" provision establishes that an EHI custodian need only *offer* two of the alternative manners, including at least one standardized manner, to avoid engaging in information blocking. 45 C.F.R. § 171.204(a)(4)(ii); *see* 89 Fed. Reg. at 1383 ("this condition has been adopted to alleviate actor uncertainty as to whether they must provide the custom build or otherwise be considered to have engaged in information blocking").

89 Fed. Reg. at 1350, extended the life of USCDI version 1 data through January 2026—when USCDI version 3 becomes the relevant standard, 89 Fed. Reg. at 1404.

The panel's opinion—which never mentions the "content and transport standard" alternative or the "part 170" certification alternative—also effectively nullifies the extensive Health IT Certification Program that HHS's Office of the National Coordinator for Health Information (ONC) offers. In addition to creating the information-blocking provisions, the Cures Act created an extensive regime geared toward increasing the interoperability of systems to seamlessly share information. Part of that regime includes defining standard data elements (like USCDI data), so they can flow easily between healthcare providers. Another part of that regime is an extensive, costly, and voluntary certification process for EHI custodians that wish to ensure that their systems comply with federal law. If compliance with these alternatives does not satisfy an actor's information blocking obligations, no EHI custodian would undertake the significant effort to obtain ONC Part 170 certification. 45 C.F.R. § 171.301(b)(1)(i). Rehearing is warranted.

II. The panel's decision contravenes both federal and state law.

Beyond misapprehending the manner exception's text, the panel's opinion also transformed the Cures Act into a litigation morass. Although the Cures Act does not create a private right of action, the panel held that a private party could sue for an alleged Cures Act violation through Maryland's unfair-competition claim. Op.37. The panel then concluded that a plaintiff adequately alleges a Cures Act violation by identifying *any* action that "is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." 42 U.S.C. § 300jj-52. It is the defendant's burden, the panel explained, to disprove the plaintiff's claim by showing that its action was required by law or expressly authorized by regulation. Op.38-39. Now, any security feature or HIPAA-mandated privacy policy may give rise to a lawsuit and costly discovery.

A. Neither Maryland nor federal law authorizes private litigants to enforce the Cures Act.

Congress declined to provide a private right of action in the Cures Act. Instead, it vested enforcement authority exclusively in the federal government. The panel upended that scheme by allowing a plaintiff to smuggle an alleged Cures Act violation into a state-law unfair-

competition claim. That holding defies the Maryland Supreme Court's reminder that "[a] private cause of action … does not exist simply because a claim is framed that a statute was violated" but rather depends on "statutory construction." *See Baker v. Montgomery County*, 50 A.3d 1112, 1122 (Md. 2012). And it conflicts with the Cures Act's design.

1. Maryland's unfair-competition law is not a blank check for private parties to enforce unrelated federal laws that lack a private right of action. A federal regulatory violation "cannot, on its own, establish defendants' liability as a matter of Maryland law." *Waypoint Mgmt. Consulting, LLC v. Krone*, 2022 WL 2528465, at *61 (D. Md. July 6, 2022). Indeed, *no* Maryland precedent supports using a federal regulatory violation as a predicate for an unfair-competition claim absent a federal private right of action.

The panel pointed to a footnote in this Court's decision in *College Loan Corp. v. SLM Corp.* for the point that the lack of a statutory private right of action alone does not "bar a plaintiff from relying on violations of that statute as evidence supporting a state law claim." 396 F.3d 588, 599 n.9 (4th Cir. 2005). That citation says nothing about whether Maryland common law supports such a claim. Instead, the decision there merely

explained that "if the Maryland common law recognized a tort based on the breach of a federally imposed standard, the [plaintiff] would be able to pursue that claim without conflicting with federal law." *Id.* at 599 n.9. But neither the panel nor RTMS found any Maryland law supporting such a novel claim, showing that such a claim is not "recognized" in Maryland.

The panel relied on *Magee v. DanSources Technical Services, Inc.*, but that case has nothing to do with unfair competition. *See* 769 A.2d 231 (Md. Ct. Spec. App. 2001). In *Magee*, the Court of Special Appeals concluded that an employee allegedly fired for refusing to defraud a federal healthcare-benefit program could maintain an *abusive discharge* claim because the relevant criminal statute did not provide any "civil remedy that would provide … redress for [retaliatory] adverse employment actions." *Id.* at 257. *Magee* says nothing about whether the Maryland Supreme Court would drastically expand Maryland's unfair-competition cause of action.

2. The Cures Act's enforcement scheme further undermines any unfair-competition claim. Under the Restatement, a state unfair-competition claim cannot be based on a statutory violation if doing

so is "inconsistent with … legislative intent." Restatement (Third) of Unfair Competition § 1, cmt. *a* (1995). The federal preemption analysis is similar, asking whether "state law stands as an obstacle to the accomplishment and execution of the full purposes of the federal law." *N. Va. Hemp & Agric., LLC v. Virginia*, 125 F.4th 472, 492-93 (4th Cir. 2025).

The panel acknowledged that claims like RTMS's could raise "genuine concerns about the predictability of the law for regulated entities." Op.35. And the panel further acknowledged that the Cures Act creates "a federal mechanism for resolving Cures Act violations." Op.36. This includes a standardized process to receive information-blocking reports, a discretionary investigation and penalty power, consultation with the Office for Civil Rights, and a nonduplication-of-penalty requirement. *See* 42 U.S.C. §§ 300jj-52(b)(1), (b)(3)(A), (d)(3), (d)(4).

But the panel failed to analyze these features of the federal enforcement regime to determine whether it evinces an intent by Congress to displace enforcement through state common law. *See Guthrie v. PHH Mortg. Corp.*, 79 F.4th 328, 339-40 & n.11 (4th Cir. 2023) (noting that this Court has repeatedly found state-law causes of action

preempted by an extensive federal enforcement regimes (citing *Anderson v. Sara Lee Corp.*, 508 F.3d 181, 182, 193-94 (4th Cir. 2007) and *Columbia Venture, LLC v. Dewberry & Davis, LLC*, 604 F.3d 824, 832 (4th Cir. 2010)). Instead, it determined that because "the Cures Act plainly contemplates that the states will regulate in this area" generally, no conflict preemption could arise. *See* Op.36. That is the wrong analysis. The question is not whether Congress has displaced states from the entire field but rather whether this claim "interfere[s] with the careful balance struck by Congress with respect to" enforcement of the Cures Act. *Arizona v. United States*, 567 U.S. 387, 406 (2012). It does.

The panel erred when it concluded that RTMS could proceed on a Maryland common-law claim. Maryland law, the constitutional-avoidance principle, and the Supremacy Clause all require the opposite result.

B. The panel inverted the burden of proof, requiring PointClickCare to disprove the information blocking claim.

On the merits and to obtain a preliminary injunction, the plaintiff has the burden of proof to establish all the elements of its claim. *See Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008). In a series

of decisions, the Supreme Court has set out a framework to determine whether a statutory exception is an element of a claim or an affirmative defense on which the defendant bears the burden of proof. *See Cook*, 84 U.S. at 173-74; *United States v. Vuitch*, 402 U.S. 62, 69-70 (1971); *Meacham v. Knolls Atomic Power Lab'y*, 554 U.S. 84, 91-95 (2008). The fundamental question is whether "the ingredients constituting the offence may be accurately and clearly defined without any reference to the exception." *Cook*, 84 U.S. at 173-74. If so, then the exception is an affirmative defense. If not, the exception is an element of the claim.

Whether an action is "information blocking" cannot be understood without reference to the exceptions. The statute specifically provides that these regulatory exceptions "do not constitute information blocking." 42 U.S.C. § 300jj-52(a)(3). And given the breadth of the information blocking prohibition, *every* EHI custodian operates within the definitional carveouts or else they would not be able to satisfy their obligations under federal privacy law.

The panel's contrary decision requiring PointClickCare "to show that its actions were not information blocking because a regulatory exception applies," Op.39—which was dispositive to its analysis because

RTMS could not have carried that burden—is both wrong and unworkable. Every EHI custodian must, *by law*, "interfere with, prevent, or materially discourage … use" of EHI, 42 U.S.C. § 300jj-52(a)(1), by controlling the dissemination of EHI to comply with HIPAA. Any rule that allows a plaintiff to pursue litigation and obtain discovery into sensitive security protocols against a custodian precisely because it is complying with federal law invites endless litigation and threatens the viability of EHI custodians.

The *en banc* court should grant review and address this issue that affects *every* American's confidential EHI. At the very least, it should grant review and hold the case pending the Supreme Court's decision in *Cunningham v. Cornell University*, No. 23-1007. In that case, the Supreme Court will address in the ERISA context whether a plaintiff must plead non-compliance with statutory exceptions, where the otherwise broad prohibition would give rise to endless litigation. The Court's analysis may be determinative here and would be new precedent the *en banc* court should consider before unleashing a wave of litigation.

III. The questions raised in this appeal are of exceptional importance.

Because of this appeal's dramatic impact on the entire healthcare community, *en banc* review is warranted. The appeal presents questions of exceptional importance that affect the compliance duties of a vast, multibillion-dollar industry tasked with safeguarding the sensitive health information of every person in the United States. By gutting the Cures Act rulemaking's regulatory text and replacing it with nebulous standards that invite repeated litigation, the panel's opinion eliminates HHS's designated standardized-access safe harbor.

That issue is particularly problematic because all exceptions to the definition of "information blocking" are set by HHS's regulations. EHI custodians cannot operate at all without certainty that they will not be haled into court by opportunistic companies doing what RTMS has done here—using the Cures Act's broad definition of "information blocking" as a crowbar to lever open EHI repositories and obtain all the data they want, however they demand, without paying for it.

The panel's errors infect every aspect of its opinion. The decision should be reconsidered and reversed.

CONCLUSION

For the foregoing reasons, PointClickCare respectfully requests that the panel or the *en banc* Court grant rehearing.

Respectfully submitted,

/s/Jeremy M. Bylund

Jeremy M. Bylund
Counsel of Record
WILLKIE FARR & GALLAGHER LLP
1875 K Street N.W.
Washington, DC 20006
(202) 303-1053
jbylund@willkie.com

Rod J. Rosenstein
Amy R. Upshaw
Joshua N. Mitchell
KING & SPALDING LLP
1700 Pennsylvania Ave. NW
Washington, DC 20006
(202) 737-0500

William C. Jackson
GOODWIN PROCTER LLP
1900 N Street NW
Washington, DC 20036
(202) 346-4216

Counsel for PointClickCare Technologies Inc.

March 26, 2025

CERTIFICATE OF COMPLIANCE

This petition complies with the type-volume limitation of Fed. R. App. P. 40(d)(3)(A), because it contains 3,891 words, excluding the parts of the petition exempted by Fed. R. App. P. 32(f).

This petition complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6), because it has been prepared in a proportionally spaced typeface using Microsoft Word 365 in Century Schoolbook 14-point font.

Date: March 26, 2025

/s/Jeremy M. Bylund
Jeremy M. Bylund

Counsel for PointClickCare Technologies Inc.

ADDENDUM

PUBLISHED

UNITED STATES COURT OF APPEALS
FOR THE FOURTH CIRCUIT

No. 24-1773

REAL TIME MEDICAL SYSTEMS, INC.,

Plaintiff - Appellee,

v.

POINTCLICKCARE TECHNOLOGIES, INC., d/b/a PointClickCare,

Defendant - Appellant.

AMERICAN HOSPITAL ASSOCIATION; ELECTRONIC HEALTH RECORD ASSOCIATION,

Amici Supporting Appellant.

Appeal from the United States District Court for the District of Maryland, at Greenbelt. Paula Xinis, District Judge. (8:24-cv-00313-PX)

Argued: January 28, 2025 Decided: March 12, 2025

Before GREGORY, WYNN, and HEYTENS, Circuit Judges.

Affirmed by published opinion. Judge Wynn wrote the opinion, in which Judge Gregory and Judge Heytens joined.

ARGUED: Jeremy Michael Bylund, KING & SPALDING LLP, Washington, D.C., for Appellant. Marie Celeste Bruce, RIFKIN WEINER LIVINGSTON, LLC, Bethesda, Maryland, for Appellee. **ON BRIEF:** William C. Jackson, GOODWIN PROCTER LLP, Washington, D.C.; Nicole Bronnimann, Houston, Texas, Rod J. Rosenstein, Amy R. Upshaw, Joshua N. Mitchell, KING & SPALDING LLP, Washington, D.C., for Appellant. Michael T. Marr, Madelaine Kramer Katz, RIFKIN WEINER LIVINGSTON, LLC, Bethesda, Maryland, for Appellee. James E. Tysse, Kelly M. Cleary, Margaret O. Rusconi, Emily I. Gerry, Stephanie Ondroff, AKIN GUMP STRAUSS HAUER & FELD LLP, Washington, D.C., for Amici Curiae.

WYNN, Circuit Judge:

Plaintiff Real Time Medical Systems, LLC[1] provides analytics services to skilled nursing facilities by accessing health records from Defendant PointClickCare Technologies, Inc., which operates a system that hosts patients' electronic health records. Real Time frequently accesses the health records in question using "bots," or automated users. PointClickCare claims that Real Time's use of bots raises security and system-performance concerns and has blocked the profiles of users whom it suspects have accessed its system using bots.

This appeal arose when Real Time sued to stop PointClickCare from restricting its access to PointClickCare's systems, and the district court granted Real Time a preliminary injunction. For the reasons that follow, we affirm.

I.

The following facts are based on the record as it comes to us on this preliminary, interlocutory appeal.

A.

Real Time is a Maryland health-analytics company that services skilled nursing facilities and other providers. Dr. Scott Rifkin founded the company more than a decade ago because, in his view, while nursing-home staff know how to look for and treat the "fires" (such as vomiting and chest pain), they are not as aware of the little signs (such as

[1] While our case caption labels Real Time as a corporation—in line with the caption in the complaint and the caption used below—Real Time's counsel clarified at oral argument that Real Time is an LLC.

fluctuations in weight or bowel movements) that could signal an impending crisis like sepsis. J.A. 392.[2] Nor do nursing homes have the staff to perform that kind of detailed monitoring.

So, Real Time aims to evaluate patients' medical records—as close to real time as possible—to look for what Dr. Rifkin calls "interventional moments." J.A. 393. When such an interventional moment arises, Real Time alerts medical staff and provides a treatment protocol. The goal is to catch a problem early, while it is easily treatable, to avoid a hospital admission and heightened risk of death.

While it is not the only company providing this service, Real Time has been particularly successful in performing this work. *E.g.*, J.A. 175–86 (affidavits and declarations from medical providers and others involved in running nursing facilities attesting to Real Time's benefits and averring that without these services their "facilities are likely, over any substantial amount of time, to see an increase in resident hospitalizations and/or deaths"). This type of analytics is a game-changer because "up until not too long ago, the data that was used to make decisions about . . . patient care in nursing homes[] was" often "30, 60, 90 days[] old"—which is helpful for making long-term, prospective decisions, but irrelevant for a patient on the verge of crisis today. J.A. 569.

A recent academic study showed that hospital readmissions significantly decreased where Real Time's program was implemented. The researchers noted that, if all skilled nursing facilities could reduce their readmissions to the rate shown for the Real Time-

[2] Citations to the "J.A." refer to the Joint Appendix filed by the parties in this appeal.

associated facilities in their study, the Centers for Medicare & Medicaid Services would save around $2.8 billion annually. Today, Real Time's customers include around 1,700 skilled nursing facilities as well as health insurers, CVS Health Corporation, and the state of Maryland.

To conduct its work, Real Time needs access to the patient's medical chart. But gone are the days of "the old paper charts that [a doctor] used to walk up and open." J.A. 417. Nowadays, charts are stored in Electronic Health Records ("EHR") systems. While there are multiple EHR companies, PointClickCare provides EHR support to more than half of nursing homes in the United States, serves 1.6 million patients at around 27,000 facilities, and hosts about 6 million users on its platform. The vast majority of Real Time's skilled-nursing-facility customers—roughly 1,400 of its 1,700 facilities, covering roughly 140,000 patients—use PointClickCare's system to host their medical records.

PointClickCare also offers medical providers various support products, such as for invoicing, and uses an automated process to push out 1.2 million medication administrations per day. And as discussed further below, for the last few years PointClickCare has been trying to enter the analytics space as another competitor to Real Time.

Medical records remain the property of the patient, even when stored on an EHR system. So, for Real Time to access the medical records necessary to conduct its analytics, it enters agreements with its customer facilities under which the patient (via the customer facility) provides Real Time with permissions and login information. PointClickCare also enters agreements with its customer facilities. Its standard agreement permits customers to

assign users (such as Real Time) to access the database. Thus, Real Time and PointClickCare have mutual customers but do not contract with each other.

Once Real Time receives login information from its customer, it regularly downloads information from PointClickCare's system to perform its analytics. Because of the amount of data needed, it uses bots to perform this task. Using humans instead would require 450 people working around the clock seven days a week just to pull the data from PointClickCare's system. *Real Time Med. Sys., Inc. v. PointClickCare Techs., Inc.*, No. 8:24-cv-00313-PX, 2024 WL 3569493, at *2 (D. Md. July 29, 2024) (citing J.A. 509–10). PointClickCare introduced testimony that it would prefer hundreds of human users to a bot because the humans would take longer to perform the task, thus spreading out the strain on the system. But Real Time's Chief Technology Officer, Christopher Miller, testified that such a setup would not be financially feasible because the cost of the staffing would exceed the fees Real Time charges its customers.

Real Time's bots download basic, standardized data, as well as a bespoke "Follow Up Questions" Report, which includes point-of-care data and is customizable by the customer. Point-of-care data is data that is "recorded generally at bedside," J.A. 453, such as "a patient's use of feeding tubes or number of bowel movements," J.A. 17. By volume, roughly 70 to 75% of the data Real Time uses for its analysis comes from the Follow Up Questions Reports.

After importing the data into its system, Real Time standardizes it, then analyzes it to look for interventional moments and pushes out alerts to providers as needed. This process is "fully automated," although humans perform routine quality-assurance

evaluations. J.A. 458.

Real Time has been using bots to pull data from PointClickCare's EHR since March 2014. Real Time has never experienced a security breach, has never been told by a governmental client that its security systems are ineffective, and has the highest security certification offered in the health-data space. It uses the same automated process with other EHR providers without issue. And PointClickCare's Senior Vice President of Software-as-a-Service Operations, Bachar Fourati, and Chief Product Officer, Robert Boyle, each conceded they were not aware of any security breach resulting from "anything Real Time has done in [PointClickCare's] system." J.A. 656; *accord* J.A. 781–82, 794.

Indeed, for roughly eight years, Real Time accessed PointClickCare's systems using bots without PointClickCare raising any concerns about the practice. True, the standard agreement that PointClickCare has used with its customers for at least five years instructed that—subject to the 21st Century Cures Act and its regulations, which are central to this case and discussed further below—"[c]ustomer[s] shall not, and shall ensure Users [like Real Time] do not," use bots to extract data or access services in a way that adversely impacts performance. J.A. 1074. But, for all those years, PointClickCare never complained to Real Time about its bot usage. None of the other EHR companies with which Real Time works have complained or suggested that Real Time's actions cause performance issues in their systems, either. Nor is there any indication PointClickCare ever sued a customer for breach of the agreement "related to usage of automated users." J.A. 653.

B.

PointClickCare began to consider competing with Real Time in the health-analytics

arena around 2020 or 2021. Shortly thereafter, it started to acquire Real Time's competitors to support this endeavor. PointClickCare's competitive product must rely on the same records Real Time accesses—and it does not restrict its *own* automated access to that data—although PointClickCare's counsel argued below that its own automated access does not pose security or performance concerns because the systems are integrated.

In 2022, the state of Maryland's health information exchange, Chesapeake Regional Information System for Our Patients ("CRISP"), put out a request for proposals. Reacting to perceived failures during the COVID pandemic, Maryland sought to "use technology to mitigate having full-blown communicable disease outbreaks in congregate care settings, specifically in nursing homes." J.A. 562. At least three companies bid on the project, including Real Time and PointClickCare. Real Time ultimately won the contract, and the program is ongoing today.

In the spring of 2022, Real Time reached out to PointClickCare, seeking to access some of PointClickCare's data directly (without the need to download) through direct integration between Real Time and PointClickCare's Marketplace Application Programming Interface ("Marketplace API"). "Within about a week," PointClickCare informed Real Time "that there wasn't a category within the marketplace that fit" or that Real Time "qualified for," but that Real Time could instead pursue direct integration through PointClickCare's "United States Core Data for Interoperability" ("USCDI") connector program. J.A. 499, 1307. Those talks ultimately fizzled out, and Real Time continued to access PointClickCare's system using bots, without complaint from PointClickCare.

Then in November 2022, without warning, PointClickCare introduced into its system a CAPTCHA wall. CAPTCHA stands for "Completely Automated Public Turing Test to Tell Computers and Humans Apart." *Real Time*, 2024 WL 3569493, at *1. "A CAPTCHA is a well-known internet security device designed to ensure that humans, not automated software or 'bots,' are attempting to gain access to the online platform." *Id.* at *2. The CAPTCHAs that PointClickCare introduced in November 2022 were the type that is often presented on today's websites, such as:

J.A. 1109; *see* J.A. 716. The text or other puzzle is meant to be decipherable by a human but difficult or impossible for a bot to solve.

PointClickCare claims it introduced the CAPTCHA wall after "numerous incidents and issues" had impacted performance and because it was "concerned about security," though it has not pointed to any specific incidents or reasons for concern preceding the introduction of the CAPTCHAs. J.A. 703. Nevertheless, after encountering the CAPTCHAs—and after hearing from a customer that PointClickCare had told the customer that Real Time was slowing down its systems—Real Time discussed the issue with

PointClickCare and reduced its data pulls from four to two times a day. PointClickCare again did not tell Real Time that it could not use bots or that bots posed a security risk. With no indication from PointClickCare that it was concerned about blocking access from *all* bots, including those controlled by a well-known entity like Real Time, Real Time "created a team tasked with manually deciphering [the] CAPTCHA images," after which its bots could perform their function. J.A. 130.

Also in November 2022, PointClickCare started an internal "watch list" of users it thought were bots based on historical usage of the system and resource consumption. J.A. 723. According to PointClickCare, users who are not on the watch list are *never* presented with CAPTCHAs, but once a user is placed on the watch list, that user will have to solve a CAPTCHA when it logs in and also when it accesses certain pages. Once a user ID is placed on the watch list, it is never taken off, and so even if a human logs in using that account, they will be faced with CAPTCHAs.

PointClickCare's witness, Fourati, waffled on what level of usage led a user to be placed on the watch list, ultimately asserting that it would be "a minimum of ten times the [usage of a] normal user," where a "normal user" makes around "500 to 1,000 requests per day." J.A. 771–72. That would mean that a user making roughly 5,000 to 10,000 requests per day should be watch-listed. However, the district court cast doubt on Fourati's testimony, noting that one of PointClickCare's few exhibits demonstrating bot activity showed a user making well over 5,000 requests per day for more than six months straight in 2023 and 2024—and at or above 10,000 requests a day for the last two and a half months—before it was apparently watch-listed.

Fourati also testified that, sometime early in 2023, PointClickCare received a customer complaint related to its system's performance. After investigating, PointClickCare discovered that, around April 5 and 6, 2023, usage from user IDs that the customer said belonged to Real Time was exceedingly high. PointClickCare introduced two graphs from those dates purporting to show this usage. Those two graphs from April 2023 are the only concrete data PointClickCare provided regarding Real Time's bots' effect on its systems,[3] *see Real Time*, 2024 WL 3569493, at *5–6, *8, even though Fourati testified that PointClickCare documents "every time there's an outage" and "track[s] all those incidents," J.A. 691.

On April 14, 2023, PointClickCare adopted an internal bot-prevention policy. However, the policy was updated twice in September 2023, and it is not clear that the most up-to-date version is available in the record. *Real Time*, 2024 WL 3569493, at *5. While the policy states that PointClickCare will send a series of warnings to customers related to

[3] In his declaration, Fourati also cited an "incident [which] involved [Real Time's] bot user submitting an extreme number of reports, making excessive database queries that caused database collapse, impacting 10,000 patients; 1,450 of which were Maryland-based patients. In that particular circumstance, it took about an hour to bring the server and database back online for PointClickCare's customers." J.A. 243. PointClickCare cites this assertion in its brief and claims that it is supported by "documentation." Opening Br. at 26; *see id.* at 18–19. In fact, PointClickCare did not introduce *any* documentary evidence for this alleged incident. Fourati's declaration did not even provide a date. Nor did he explain how he knew the user in question was associated with Real Time. Moreover, he did not mention this incident at all in his testimony at the hearing, despite spending significant time discussing alleged bot-related performance issues. Rather, when asked whether the two graphs from April 2023 were "all that[was] in [his] affidavit [sic] as far as Real Time," Fourati responded, "Yeah, that's fair." J.A. 803. Finally, counsel also did not point to this alleged incident during the motion argument below. We thus follow the district court's lead and do not consider this unsupported allegation.

bot usage, there is no evidence it ever did so. Nor does the policy include any objective criteria related to what level of usage triggers a user's placement on the watch list.

Around May 2023, Real Time and PointClickCare entered potential merger and acquisition talks and, on May 31, executed a non-disclosure agreement ("NDA"). In mid-June, pursuant to the NDA, Real Time began executing a premerger information exchange, under which it "pretty much shared everything with [PointClickCare]" related to its data-analytics methodology, customers, and finances. J.A. 408. Real Time also gave PointClickCare a demonstration of its product. Although it was clear during these discussions that Real Time's business model was built around bots, PointClickCare yet again did not raise concerns about security during these talks. Real Time's Chief Strategy and Development Officer, Timothy Buono, testified that after the parties discussed Real Time's security certification, "that was the end of the discussion at least related to security," as far as he could recall. J.A. 589.

In early October 2023, however—again without warning—PointClickCare escalated its CAPTCHA process by introducing indecipherable CAPTCHA images, such as:

J.A. 130. "Real Time's [human] operators were largely unsuccessful at deciphering these new CAPTCHA images[.]" J.A. 131. By definition, CAPTCHAs are meant to be solvable

by humans, so an indecipherable image is technically no longer a "CAPTCHA." For ease of reference, however, and consistent with the practice of the parties and the district court, we will refer to these images as "indecipherable" or "unsolvable" CAPTCHAs.

At the same time, PointClickCare began blocking users if (or rather, when) they could not solve its unsolvable CAPTCHAs. Once one of its users was blocked, Real Time had to ask its customer to reset the account—only to be faced with CAPTCHAs again and, after again failing, end up being re-blocked. This wasted the time of both Real Time and its customers. Moreover, "the introduction of [the] new images resulted in Real Time being unable to retrieve [Follow Up Questions] Reports for dozens of Nursing Facilities," with Real Time's access to data for at least seventy-five nursing facilities being "adversely impacted," including its access for twenty-one Maryland nursing facilities being "entirely severed." J.A. 131.

It was only at this point that Real Time learned PointClickCare was not interested in pursuing acquisition. *See Real Time*, 2024 WL 3569493, at *3 ("Acquisition talks appear to have continued long enough for [PointClickCare] to learn of Real Time's business details without sharing any of its own."). PointClickCare never provided Real Time a reason for cutting off the acquisition talks.

The indecipherable CAPTCHAs were "turned off" for a few days in late October 2023. *Id.* at *4 (citing J.A. 134). But by early November, they were back, and Real Time's users at "over 700 of [its] 1400 facilities that utilized PointClickCare[']s system] were fully locked out." J.A. 474.

C.

Faced with this pressing issue, Real Time sought a solution with PointClickCare. It reduced the volume of its data pulls by half yet again, cutting them to "just once a day" and running them overnight, both to get as complete a picture of the day as possible and "as a gesture of good will, to try to just be in the system when fewer users are." J.A. 451–52.

The parties discussed whether Real Time could join PointClickCare's Marketplace API. But there were two issues with this approach: first, the Marketplace would include only about 30% of the data Real Time needed; and second, PointClickCare wanted Real Time to sign its standard marketplace agreement in order to join the Marketplace API, but the agreement included numerous terms Real Time found objectionable, including a requirement that it not develop or commercialize products that PointClickCare deemed, in its "sole discretion," to be "directly competitive" to its own products. J.A. 133. Given that PointClickCare was by now a competitor to Real Time's health-analytics product, Real Time believed it would have been "immediately" in breach of any such agreement. J.A. 593.

The parties also again discussed USCDI connector access, but, like the Marketplace API, the USCDI would provide less than 30% of the needed data, which "would be insufficient to produce or provide value." J.A. 455; *see* J.A. 509. Another possible avenue for obtaining data, called a "data relay," would provide a data export to the customer nursing facility, which Real Time could then obtain from the customer. J.A. 515. However, it, too, "would [provide] under 30 percent of the data . . . volume that [Real Time] work[s] with" because it would lack point-of-care data unless the parties negotiated to include it.

J.A. 516. Even then, however, it would pose an issue because the data would be provided directly to the nursing facilities, most of which do not have the technical capability to provide it to Real Time in a usable format.

Faced with these hurdles, technical employees within both companies began an initially productive dialogue regarding an alternative solution: Real Time would join the Marketplace API, and PointClickCare would export the data not available via the Marketplace API, either sending it to Real Time through a secure method or "stor[ing] [it] for [Real Time] to securely retrieve." J.A. 473.

Chief Technology Officer Miller testified that Real Time would prefer to get its data in this way, which would allow it to receive the data "in one big . . . bunch" rather than having to run bots to download the needed data. J.A. 512. Real Time's Chief Information Security Officer, Andrew Lister, explained that it has such an arrangement with another company with which it works for four of its nursing-facility customers. He testified that this arrangement "tells [Real Time] that it's feasible to do and not that difficult to do, and it doesn't take that long . . . to even set it up or even run it," based on his conversations with that other company. J.A. 535. Further, this solution would resolve PointClickCare's cited security and system-degradation concerns related to Real Time's bot usage by eliminating the need for bots.

The parties' technical employees began developing the "connector to the API," and got about a third of the way through that process. J.A. 468. Meanwhile, Chief Strategy and Development Officer Buono suggested to PointClickCare that the parties "draft an agreement from scratch," but PointClickCare "insisted that [Real Time] mark up

[PointClickCare's standard marketplace] agreement." J.A. 591. So, on November 29, Real Time sent redlines to the Marketplace API agreement that it indicated would resolve its concerns with the contract.[4] Real Time also proposed a fee structure for the combined Marketplace and data-export solution.[5]

But then PointClickCare suddenly ceased communicating about this possible solution. Miller testified that PointClickCare's communications "just stopped. . . . I would occasionally ask a question, they were quick to respond, spin up a phone call. But I became aware that there was a breakdown. We were told we weren't going to get what we had been discussing, and so it just simply stopped." J.A. 474. PointClickCare never indicated to Real Time that there were any technical barriers to the proposed data export or Marketplace API connection. Nor did it respond to Real Time's proposed redlines to the Marketplace API agreement or to its fee proposal.

Instead, on December 14, 2023, PointClickCare simply informed Real Time that it did not intend to pursue the agreement: it "would not entertain any changes to the marketplace agreement"; the data "extracts would not be made available"; and "[t]he use

[4] One of the redlines Real Time made to the agreement was to strike the prohibitions on Real Time's use of bots. However, Buono testified that if Real Time could get the needed information through a combination of the Marketplace API and data extracts, he "would imagine" the prohibition on bots "would be a non-issue." J.A. 610.

[5] The precise fee proposal is not clear from the record. The parties agree that PointClickCare requests $65 per facility per month for regular access to the Marketplace API, or $125 per facility per month for premium access, which appears to include at least some items not relevant here. Buono testified that Real Time's initial counteroffer was $30 and $60, respectively. Later, however, he testified that Real Time had countered with an offer of $70 to cover the information it was requesting. Thus, when PointClickCare's lawyer asked whether $65 was unreasonable, he said that it was not, as Real Time had "countered with $70." J.A. 607.

of data relay would not be made available . . . as a potential solution," nor would PointClickCare "agree to any changes" to the data-relay output. J.A. 594. PointClickCare also notified Real Time that it did not intend to give Real Time a demonstration of its product pursuant to the NDA.

Two of Real Time's witnesses testified that PointClickCare executives told them that PointClickCare was not interested in collaboration because it felt it could outcompete Real Time. *See* J.A. 409–10 (Dr. Rifkin testifying that PointClickCare's senior vice president, Travis Palmquist, told him this); J.A. 594–95 (Buono testifying that PointClickCare's vice president of partnerships and strategic alliances, Marino Cherubin, told him this); *see also* J.A. 162 (Buono's affidavit). PointClickCare denies that its executives made such statements—and notes that it works with other competitors—but has not provided any explanation for why it ceased talks.

For example, while Buono testified that Cherubin told him that PointClickCare "would not entertain any changes to the [M]arketplace [API] agreement," J.A. 594, Cherubin conceded that the agreement was normally "subject to modification through negotiation," J.A. 858–59, and that when PointClickCare entered into data-exchange agreements with other companies—including three he identified as competitors—"there were modifications to the agreement," J.A. 852. Yet, Cherubin admitted, PointClickCare simply "did not respond" to Real Time's redline of the agreement. J.A. 859.

Having failed to reach a business resolution, Real Time sued PointClickCare in Maryland state court on January 9, 2024. It asserted seven claims, of which two are relevant on appeal: unfair competition (Count II) and tortious interference with Real Time's

contracts with the skilled nursing facilities (Count IV). Among other relief, it sought an injunction to stop PointClickCare from using the indecipherable CAPTCHA images and deactivating Real Time's accounts. PointClickCare quickly removed the case to federal court[6] and then moved to dismiss for failure to state a claim.

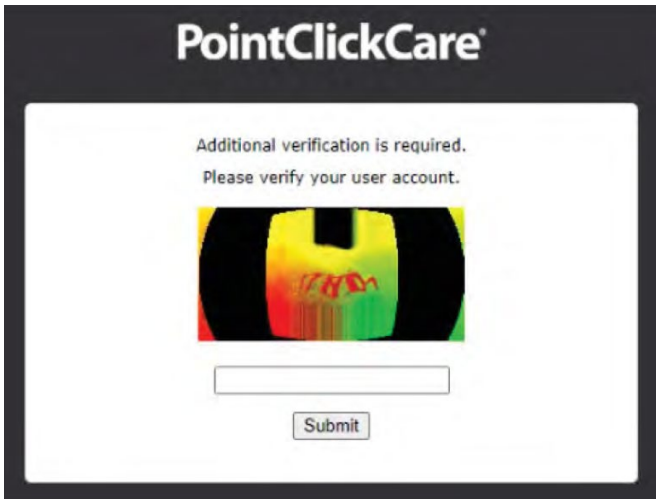
---

[6] In its notice of removal, PointClickCare invoked both federal question jurisdiction and diversity jurisdiction. Notice of Removal at 1, *Real Time*, No. 8:24-cv-00313-PX (D. Md. Jan. 31, 2024), ECF No. 1. Whether this case implicates a federal question is a complicated question. *See Republican Nat'l Comm. v. N.C. State Bd. of Elections*, 120 F.4th 390, 400 (4th Cir. 2024) (describing the applicable four-part test); *Burrell v. Bayer Corp.*, 918 F.3d 372, 376 (4th Cir. 2019) (noting that "federal jurisdiction over state-law causes of action" lies "only in a special and small class of cases" (internal quotation marks omitted)). We need not resolve that issue because we conclude that the federal courts possess diversity jurisdiction over this matter. *See* 28 U.S.C. § 1332(a)(2).

PointClickCare asserted in its notice of removal that it "is incorporated in Ontario, Canada and maintains its principal place of business in Ontario, Canada." Notice of Removal at 5; *accord* J.A. 12 (complaint alleging that PointClickCare "a foreign corporation, with its principal place of business" in Ontario, Canada, and "is registered to do business in Minnesota"). The notice of removal also correctly identified Real Time as an LLC. "For purposes of diversity jurisdiction, the citizenship of a limited liability company . . . is determined by the citizenship of all of its members[.]" *Cent. W. Va. Energy Co. v. Mountain State Carbon, LLC*, 636 F.3d 101, 103 (4th Cir. 2011). But the notice of removal indicated that PointClickCare was "unaware of the identities of [Real Time's] member(s) and therefore their place(s) of citizenship." Notice of Removal at 5. That is insufficient. *See Moses Enters., LLC v. Lexington Ins. Co.*, 66 F.4th 523, 526 n.1 (4th Cir. 2023) (noting a defect where "the complaint contains no mention of [an LLC's] members' citizenships"); *Ellenburg v. Spartan Motors Chassis, Inc.*, 519 F.3d 192, 200 (4th Cir. 2008) (stating that the removing party is held to same pleading standard as plaintiff filing initial complaint); *accord Stewart v. Gruber*, No. 23-30129, 2023 WL 8643633, at *2 (5th Cir. Dec. 14, 2023) (per curiam) (faulting removing defendants for not identifying citizenship of plaintiff LLC's members); *Roberts v. Nix*, No. 1:22-cv-00235, 2022 WL 4372086, at *4 (S.D. W. Va. Sept. 21, 2022) (same).

However, "28 U.S.C. § 1653 allows '[d]efective allegations of jurisdiction' to 'be amended' on appeal." *Moses Enters.*, 66 F.4th at 526 n.1. And "[a]t oral argument, [counsel for Real Time] asserted, without contradiction"—and in consultation with her client—that none of Real Time's members are residents of Canada. *Thompson v. Ciox Health, LLC*, 52 F.4th 171, 173 n.1 (4th Cir. 2022); *see* Oral Arg. at 15:50–16:22, https://www.ca4.uscourts.gov/OAarchive/mp3/24-1773-20250128.mp3. "Treating that

Soon after Real Time filed suit, sometime in February 2024, PointClickCare's usage of indecipherable CAPTCHA images and blocking of Real Time's accounts slowed to a trickle for several months. Then, in mid-May 2024, Real Time saw the "return of some of the indecipherable CAPTCHAs" in larger numbers, J.A. 477, and even more indecipherable images appeared, such as this one:



J.A. 1108. PointClickCare introduced testimony that it had implemented a system whereby watch-listed users would face an initial, regular, solvable CAPTCHA; if the user could not solve that CAPTCHA, they would be faced with increasingly difficult CAPTCHAs until they reached an unsolvable one, and eventually were locked out. (Real Time put forward testimony contending that it was sometimes locked out even if it *did* happen to solve one of the more challenging CAPTCHAs.) PointClickCare explained that, at that point, even if the user reset their account and tried to log in with a human user, they would always be

uncontested allegation as a constructive amendment of the complaint under 28 U.S.C. § 1653, we are satisfied the district court had jurisdiction to consider" the preliminary-injunction proceedings. *Thompson*, 52 F.4th at 173 n.1.

brought straight to the unsolvable CAPTCHA. This new process caused Real Time to rapidly lose access to its accounts for more than 600 of its skilled-nursing-facility customers.

So, on May 30, 2024, Real Time filed the motion for a preliminary injunction at issue in this appeal. It indicated that it had no problem with decipherable CAPTCHAs, but that PointClickCare's use of indecipherable CAPTCHAs and practice of locking out accounts posed a significant threat to Real Time's ability to provide its services. In response, PointClickCare paused the indecipherable CAPTCHAs for Real Time's users, instead presenting them only with the first-level, normal CAPTCHAs.[7] But PointClickCare informed the district court that, if the preliminary injunction was denied, it would continue to use indecipherable CAPTCHAs and lock out suspected bot users.

To facilitate PointClickCare pausing the use of indecipherable CAPTCHAs for Real Time's users, Real Time sent PointClickCare a list of 572 of its users, and PointClickCare determined that 119 of those users were on the watch list (out of 570 total users on the watch list). Real Time's counsel represented, however, that the list of 572 Real Time user IDs it sent did not include "ones that were [already] locked out." J.A. 714. Our own review of the lists supports this assertion and suggests that at least *131* users on the watch list,

[7] To be sure, Real Time introduced two videos from early June in which humans sought to log in with watch-listed usernames, were faced with indecipherable CAPTCHAs, and were ultimately locked out. However, we are not aware of evidence that Real Time has had any issues logging in since the district court granted the preliminary injunction.

rather than 119, belong to Real Time.[8] It is therefore unclear from the present record what percentage of the watch list is made up of Real Time users, but it appears to be nearly a quarter at minimum.

After receiving numerous exhibits and holding a motion hearing across two full days, the district court granted the preliminary injunction on July 29. *Real Time*, 2024 WL 3569493, at *1. PointClickCare timely appealed and successfully moved this Court to accelerate the briefing schedule. Two organizations, the Electronic Health Record Association and the American Hospital Association, filed a joint Amicus Brief in support of PointClickCare's appeal. We have jurisdiction over this interlocutory appeal pursuant to 28 U.S.C. § 1292(a)(1).

II.

To begin, the district court did not determine whether Real Time sought, through an injunction, to preserve or alter the status quo. *Real Time*, 2024 WL 3569493, at *6. Preliminary injunctions that alter the status quo are known as "mandatory preliminary injunctions" and are highly disfavored. *Pierce v. N.C. State Bd. of Elections*, 97 F.4th 194,

[8] Reviewing the full watch list and identifying those usernames that directly referenced Real Time (by including something like "realtime" or "rtime") or used an individual's name included in user IDs on Real Time's list (such as D. Lister or P. Charles), we identified 128 suspected Real Time users on the full watch list. Of those 128 users that appear to belong to Real Time and are on the full watch list, only 116 were on the list of non-locked-out users that Real Time sent to PointClickCare. In other words, there appear to be at least 12 additional users associated with Real Time that were watch-listed beyond the 119 on Real Time's list. There may well be more, as we could only search the full watch list for those names clearly associated with Real Time.

209 (4th Cir. 2024). The district court concluded it did not need to resolve the issue because it would reach the same result either way. *Real Time*, 2024 WL 3569493, at *6.

Whatever the merits of that determination, we are convinced this case involves a normal, status-quo-maintaining preliminary injunction, not a mandatory one. "We have defined the status quo for this purpose to be 'the last uncontested status between the parties which preceded the controversy.'" *League of Women Voters of N.C. v. North Carolina*, 769 F.3d 224, 236 (4th Cir. 2014) (quoting *Pashby v. Delia*, 709 F.3d 307, 320 (4th Cir. 2013)).

Here, the "last uncontested status" existed before PointClickCare's October 2023 introduction of indecipherable CAPTCHAs and blocking users that failed them. Immediately after that shift in PointClickCare's practices, Real Time sought to resolve the issue directly with PointClickCare; when that failed, it sued. Shortly thereafter, the indecipherable CAPTCHAs slowed to a trickle for several months. Once they reemerged in May, Real Time rapidly moved for a preliminary injunction. Real Time thus consistently challenged the use of the indecipherable CAPTCHAs and the blocking policy, and requested the court's intervention as soon as it became clear that PointClickCare intended the policy to stay.

"To win . . . a preliminary injunction, [p]laintiffs must demonstrate that (1) they are likely to succeed on the merits; (2) they will likely suffer irreparable harm absent an injunction; (3) the balance of hardships weighs in their favor; and (4) the injunction is in the public interest." *League of Women Voters*, 769 F.3d at 236 (citing *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008)). "Although [p]laintiffs need not establish a

certainty of success, they must make a clear showing that they are likely to succeed at trial." *Roe v. Dep't of Def.*, 947 F.3d 207, 219 (4th Cir. 2020) (cleaned up).

The standard for a plaintiff to receive a preliminary injunction—even one merely seeking to preserve the status quo—is thus steep. But that does not mean the defendant has no role to play. While plaintiffs bear the burden of demonstrating each of the four preliminary-injunction elements, "the burdens at the preliminary injunction stage track the burdens at trial"—meaning, for example, defendants must shoulder the burden of proving an affirmative defense, even at the preliminary-injunction stage. *Gonzales v. O Centro Espirita Beneficente Uniao do Vegetal*, 546 U.S. 418, 429 (2006); *accord Ramirez v. Collier*, 595 U.S. 411, 425 (2022) (describing burden-shifting analysis under the Religious Land Use and Institutionalized Persons Act and noting that "[t]his allocation of respective burdens applies in the preliminary injunction context").

Further, arguments that a defendant might make on appeal from an order granting a preliminary injunction are subject to the same rules as with any appellant: we may deem an argument not properly before us if the defendant fails to sufficiently raise it before the district court or in its opening brief. *E.g.*, *Miranda v. Garland*, 34 F.4th 338, 350 (4th Cir. 2022) (defendant appealing grant of preliminary injunction failed to preserve argument by making only "cursory," footnoted reference to it); *Metro. Reg'l Info. Sys., Inc. v. Am. Home Realty Network, Inc.*, 722 F.3d 591, 602 n.13 (4th Cir. 2013) (defendant appealing grant of preliminary injunction failed to preserve argument by raising it for the first time in its reply brief); *U.S. Dep't of Lab. v. Wolf Run Mining Co.*, 452 F.3d 275, 283 (4th Cir. 2006)

(defendant appealing grant of preliminary injunction failed to preserve argument by failing to raise it before district court).[9]

"We review the decision to grant or deny a preliminary injunction for an abuse of discretion. Abuse of discretion is a deferential standard, and we may not reverse so long as the district court's account of the evidence is plausible in light of the record viewed in its entirety. A clear error in factual findings or a mistake of law is grounds for reversal." *Roe*, 947 F.3d at 219 (cleaned up).

III.

With these standards in mind, we turn to an analysis of the preliminary injunction in this case. We begin with the question of whether Real Time has demonstrated a sufficient likelihood of success on the merits. We agree with the district court that it has.

"Although the Complaint alleges six causes of action, Real Time presse[d] only three claims for purposes of injunctive relief: tortious interference with business relations, unfair competition, and breach of contract as a third-party beneficiary." *Real Time*, 2024

[9] Some of our prior cases, including those cited here, "use 'waiver' and 'forfeiture' interchangeably, but the terms technically have different meanings. 'Forfeiture' refers to a party's inadvertent failure to raise an argument; a court has discretion to reach a forfeited issue. By contrast, 'waiver' refers to a knowing, and intelligent decision to abandon an issue. Unlike a forfeited issue, a court does not have discretion to reach an issue that a party has waived." *Stokes v. Stirling*, 64 F.4th 131, 136 n.3 (4th Cir.) (citations omitted), *cert. denied*, 144 S. Ct. 377 (2023).

WL 3569493, at *7. The district court only addressed the first two claims and concluded that Real Time was likely to succeed on both. *Id.*

We agree as to the unfair-competition claim, so we need not analyze the tortious-interference claim. *E.g.*, *Roe*, 947 F.3d at 219 (affirming order granting preliminary injunction where "[t]he district court did not err in concluding that [the p]laintiffs are likely to succeed on the merits of at least one claim").

A.

When faced with a question of state law, we must look to decisions of the state's highest court and, if those decisions do not resolve the matter, "'predict' how [that] court would rule on the state law issue in question." *Koppers Performance Chems., Inc. v. Argonaut-Midwest Ins. Co.*, 105 F.4th 635, 640 (4th Cir.) (quoting *Knibbs v. Momphard*, 30 F.4th 200, 213 (4th Cir. 2022)), *cert. denied*, 145 S. Ct. 570 (2024). "In doing so, the decisions of [state] intermediate appellate courts 'constitute the next best indicia of what state law is,'" although those "decisions are never binding and 'may be disregarded if the federal court is convinced by other persuasive data that the highest court of the state would decide otherwise.'" *Colo. Bankers Life Ins. Co. v. Acad. Fin. Assets, LLC*, 60 F.4th 148, 154 (4th Cir. 2023) (quoting *Priv. Mortg. Inv. Servs., Inc. v. Hotel & Club Assocs., Inc.*, 296 F.3d 308, 312 (4th Cir. 2002)). Other forms of data to consider include "the canons of construction, restatements of the law, treatises, recent pronouncements of general rules or

policies by the state's highest court, well considered dicta, and the state's trial court decisions." *Moore v. Equitrans, L.P.*, 27 F.4th 211, 220 (4th Cir. 2022) (cleaned up).

There is no specific test for a claim of unfair competition under Maryland common law. *ClearOne Advantage, LLC v. Kersen*, --- F. Supp. 3d ---, No. 23-cv-03446-JKB, 2024 WL 4754051, at *6 (D. Md. Nov. 12, 2024); *accord Command Tech., Inc. v. Lockheed Martin Corp.*, No. 0469 Sept. Term 2014, 2015 WL 6470277, at *8 (Md. Ct. Spec. App. Oct. 27, 2015) (referring to the tort's "amorphous contours"). Rather, the Supreme Court of Maryland "has preserved a high degree of flexibility in the law of unfair competition." *Delmarva Sash & Door Co. of Md. v. Andersen Windows, Inc.*, 218 F. Supp. 2d 729, 733 (D. Md. 2002). It is defined, generally, as "damaging or jeopardizing another's business by fraud, deceit, trickery or unfair methods of any sort," and must be evaluated case-by-case. *Balt. Bedding Corp. v. Moses*, 34 A.2d 338, 342 (Md. 1943).

The prototypical unfair-competition case involves alleged violation of a business's trademark. *E.g.*, *Scotch Whisky Ass'n v. Majestic Distilling Co.*, 958 F.2d 594, 597 (4th Cir. 1992). However, the Supreme Court of Maryland[10] has long made clear the tort extends beyond that context.

For example, in 1943, it explained that, "[e]xpressed in simple words, [the purpose of the doctrine of unfair competition] was to prevent dealings based on deceit and dishonesty, and was, at first,—approximately a hundred years ago,—applied only to what

[10] "In 2022, . . . Maryland changed the name of its highest court from the Court of Appeals of Maryland to the Supreme Court of Maryland. We use the current name." *Kim v. Bd. of Educ. of Howard Cnty.*, 93 F.4th 733, 739–40 n.6 (4th Cir. 2024).

were then termed 'trade mark cases.' Since that time the gradual tendency of the Courts has been to extend the scope of the law to all cases of unfair competition in the field of business." *Balt. Bedding Corp.*, 34 A.2d at 342. So, for example, this Court has previously upheld a jury verdict finding Maryland unfair competition based on interference in product-distribution contracts. *Trimed, Inc. v. Sherwood Med. Co.*, 977 F.2d 885, 890–91 (4th Cir. 1992); *cf. Paccar Inc. v. Elliot Wilson Capitol Trucks LLC*, 905 F. Supp. 2d 675, 691–92 (D. Md. 2012) (noting that *Trimed* "strongly suggests that a finding of unfair competition can be based on an array of actions that interfere with vital aspects of business, such as customer relations, product shipments, or pricing").

"In making a case-specific determination as to whether conduct constitutes unfair competition, courts must be careful to protect legitimate competition among business rivals. . . . Business torts do not exist to allow courts to retroactively pick winners and losers in the marketplace but to enforce only minimum standards of conduct." *Command Tech.*, 2015 WL 6470277, at *8–9 (citing *Edmondson Vill. Theatre v. Einbinder*, 116 A.2d 377, 382 (Md. 1955)). "[T]he courts are solicitous to prevent unfair competition in business, and to protect against unfair practices those persons who have established and developed a business or product stamped in the public mind with the impress of the builder's skill or reputation; but the courts are equally solicitous to encourage fair competition and thereby protect the public against the evils of monopolies." *Edmondson Vill. Theatre*, 116 A.2d at 382. For this reason, Maryland's highest court has noted, "[t]he courts must be careful to guard against extending the meaning of 'unfair competition' to cover acts which may be unethical yet not illegal." *Id.*

However, as this Court has previously explained in reviewing this case law, Maryland "has never required *an unlawful act* as an essential element of an unfair competition claim." *Trimed*, 977 F.2d at 891 (emphasis added) (first citing *Balt. Bedding Corp.*, 34 A.2d at 342; then citing *Edmondson Vill. Theatre*, 116 A.2d at 382; and then citing *Cavalier Mobile Homes, Inc. v. Liberty Homes, Inc.*, 454 A.2d 367, 374 (Md. Ct. Spec. App. 1983)) (rejecting defendant's argument "that the [jury] instructions were contrary to Maryland law because, essentially, they permitted the jury to find unfair competition from lawful, competitive conduct"). Instead, we apparently understood the Maryland courts' reference to an "illegal" act to mean merely that the action must meet a certain threshold to qualify as tortious unfair competition—not that the action must be illegal under another source of law. *Cf. Command Tech.*, 2015 WL 6470277, at *8 (finding no unfair competition where the defendant "never had a legal obligation to any party" to take the sought-after action "and, thus, did not unfairly take advantage of any party's reasonable expectations").

In any event, in this case, Real Time *does* argue that PointClickCare's use of indecipherable CAPTCHAs and choice to block certain users is illegal under another source of law:[11] the information-blocking provision of the federal 21st Century Cures Act

[11] It seems the question could just as easily be framed as Real Time pointing to a tortiously unfair act, and PointClickCare raising compliance with the Cures Act as a *defense* to show that its behavior is by definition not unfair. *Cf.* Amicus Br. at 29 (conceding that "the *conduct underlying* an information blocking violation can be used to prove the elements of a Maryland common law claim, including an unfair competition . . . claim, in an appropriate circumstance"). Nevertheless, we follow the parties' framing of the issue.

of 2016 ("Cures Act"). *See* 21st Century Cures Act, Pub. L. No. 114-255, § 4004, 130 Stat. 1033, 1176–80 (2016) (codified as amended at 42 U.S.C. § 300jj-52). "Thus, says Real Time, [PointClickCare] has competed unfairly by severing Real Time's ability to provide analytics for no legitimate purpose other than to gain an economic advantage in Real Time's market." *Real Time*, 2024 WL 3569493, at *7.

PointClickCare responds that Real Time cannot rely on a violation of the Cures Act to support a claim of unfair competition under Maryland law; that even if it can, PointClickCare did not violate the Cures Act; and that even if it did, Real Time's claims fail for other reasons. We disagree on each point, which we consider in turn.

B.

PointClickCare first contends that Real Time cannot rely on a Cures Act violation to support a Maryland unfair-competition claim. This argument has two subparts: PointClickCare argues that (1) a federal statute lacking a private right of action cannot support a Maryland unfair-competition claim; and (2) the Cures Act preempts any state-law claim.

PointClickCare has failed to preserve both arguments. It failed to preserve the first by failing to present it below. *See Wolf Run Mining Co.*, 452 F.3d at 283. And it failed to preserve the second by taking only a "passing shot" at the issue in its opening brief. *Mod. Perfection, LLC v. Bank of Am., N.A.*, 126 F.4th 235, 240 n.1 (4th Cir. 2025); *see Miranda*, 34 F.4th at 350–51; Opening Br. at 61 (devoting a two-sentence paragraph to the matter). Nevertheless, because Real Time does not invoke forfeiture or waiver, both arguments have been addressed in the briefs on appeal (including briefing from Amici), and this

appeal's preliminary posture means that these matters are likely to be brought to the district court on remand, we exercise our discretion to review the arguments. *Stokes v. Stirling*, 64 F.4th 131, 136 n.3 (4th Cir.) ("[A] court has discretion to reach a forfeited issue."), *cert. denied*, 144 S. Ct. 377 (2023); *see also Jordan v. Large*, 27 F.4th 308, 312 n.4 (4th Cir. 2022) (this Court "can look" at waived arguments when "the waiver itself has been waived"); *United States v. Newby*, 91 F.4th 196, 200 n.* (4th Cir. 2024) (an appellee that fails to assert forfeiture in its brief "has forfeited any such forfeiture argument" in turn).

1.

The first question is whether a Maryland claim for unfair competition can be premised in part on a federal statute that both parties agree lacks a private right of action. We conclude it can.

In our 2005 decision in *College Loan Corp. v. SLM Corp.*, we held that "the lack of a [federal] statutory private right of action does not, in and of itself, bar a plaintiff from relying on violations of that statute as evidence supporting a state law claim." *Coll. Loan Corp. v. SLM Corp.*, 396 F.3d 588, 599 n.9 (4th Cir. 2005) (citing *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 487 (1996) (opinion of Stevens, J.) (violation of federal statute without "an implied private right of action" could support a state common-law cause of action)). We therefore rejected the notion that a plaintiff "was not entitled to utilize evidence that [a defendant] had violated [a federal statute lacking a private right of action] and its regulations to satisfy elements of its state law claims." *Id.* at 597. "To the contrary," we elaborated, "the Supreme Court (and this Court as well) has recognized that the availability of a state law claim is even *more* important in an area where no federal private right of

action exists." *Id.* at 598 (first citing *Worm v. Am. Cyanamid Co.*, 970 F.2d 1301, 1308 (4th Cir. 1992); and then citing *Silkwood v. Kerr-McGee Corp.*, 464 U.S. 238, 251 (1984)); *see also Burrell v. Bayer Corp.*, 918 F.3d 372, 377 (4th Cir. 2019) (noting state law could provide remedies despite lack of federal private right of action).

To be sure, more recently, we have explored the limits of this principle. In *Bauer v. Elrich*, we concluded that the plaintiffs could not "circumvent[]" the lack of a private right of action in a federal statute "by invocation of a state's law of taxpayer standing." *Bauer v. Elrich*, 8 F.4th 291, 295 (4th Cir. 2021). But in that case, the claim "at its core" sought to "enforce a federal statute"; the plaintiffs "d[id] not seek to advance any state law right or enforce any duty established under state law." *Id.* at 297. We concluded that the state "taxpayer standing doctrine does not grant any *substantive* rights to . . . taxpayers, but merely confers standing in state court for taxpayers to enforce a right or obligation imposed by some other provision of law." *Id.* at 298 (emphasis added). Thus, we rejected the plaintiffs' contention that the alleged "violation of federal law merely [was] an element of their cause of action authorized under [state] law." *Id.* Rather, "[b]ecause federal law create[d] the substantive requirement that the plaintiffs [sought] to enforce, we look[ed] to federal law to determine whether a private remedy [was] authorized" (which it was not). *Id.* at 299.

In so ruling, we relied on a Supreme Court decision establishing that plaintiffs cannot avoid the absence of a private right of action in a federal statute merely by seeking to enforce compliance with that statute as a provision of a contract to which the plaintiff claimed to be a third-party beneficiary. *Id.* at 299–300 (citing *Astra USA, Inc. v. Santa*

Clara County, 563 U.S. 110, 113–14, 116–18, 119 n.4 (2011)). We noted that "[t]he Supreme Court declined the plaintiff's attempt to bring a breach of contract claim that was '*in substance one and the same*' as a suit to enforce the governing statute directly." *Id.* at 300 (emphasis added) (quoting *Astra USA*, 563 U.S. at 114). Nevertheless, we did not purport to overrule *College Loan Corp.*; to the contrary, we recognized that some of our prior cases had allowed "federal standards merely [to] serve[] as evidence that the state law duty had been violated." *Id.* at 301. And we have continued to rely on the relevant portion of *College Loan Corp.* after *Bauer*. *E.g.*, *Guthrie v. PHH Mortg. Corp.*, 79 F.4th 328, 340 (4th Cir. 2023) (citing *College Loan Corp.*, 396 F.3d at 597–99), *cert. denied*, 144 S. Ct. 1458 (2024).

In sum, our case law establishes that it is acceptable to use a violation of a federal statute as evidence supporting a state law claim—but not to advance a state claim that is merely a shell for an otherwise-unavailable federal claim.

The claim Real Time advances falls squarely in the "acceptable" camp. Real Time does not seek merely to enforce the Cures Act on its own terms, using state law to evade the lack of a private right of action under federal law. Rather, it seeks to use a violation of the Cures Act as evidence to support an element of a larger state-law claim for unfair competition—that is, to show that certain actions taken by its competitor are unfair and wrongful. That is permissible under our precedent.

It also appears to us that the Supreme Court of Maryland would permit such a claim to proceed. Again, Maryland unfair competition is a highly "flexib[le]" tort, *Delmarva Sash & Door Co.*, 218 F. Supp. 2d at 733, which is to be evaluated case-by-case, and which

seeks to prevent competitors from using "fraud, deceit, trickery *or unfair methods of any sort*" to "damag[e] or jeopardiz[e] another's business," *Balt. Bedding Corp.*, 34 A.2d at 342 (emphasis added). And Maryland's intermediate appellate court has allowed a plaintiff pursuing a different state tort to point to a federal law lacking a private right of action. *See Magee v. DanSources Tech. Servs., Inc.*, 769 A.2d 231, 257 (Md. Ct. Spec. App. 2001) ("[The plaintiff]'s evidence of [federal] health care benefit fraud satisfied the second 'unvindicated public policy mandate' element of a[state] abusive discharge cause of action.").

Moreover, whether a party "had a legal obligation" to take (or not take) a certain action can inform the unfair-competition analysis under Maryland law. *Command Tech.*, 2015 WL 6470277, at *8; *cf. Goldman v. Harford Rd. Bldg. Ass'n*, 133 A. 843, 846 (Md. 1926) ("Competition is the state in which men live and is not a tort, unless the nature of the method employed is not justified by public policy, and so supplies the condition to constitute a legal wrong."). Maryland case law makes clear that this legal obligation can arise from federal law. *E.g.*, *Barnett v. Md. State Bd. of Dental Exam'rs*, 444 A.2d 1013, 1022 (Md. 1982) (relying on the federal Lanham Act). And the fact that the Cures Act does not include a private right of action does not mean that its information-blocking provision does not impose a "legal obligation" on PointClickCare; it undisputedly does. *Cf. Intus Care, Inc. v. RTZ Assocs., Inc.*, No. 24-cv-01132-JST, 2024 WL 2868519, at *2 (N.D. Cal. June 5, 2024) (concluding that a Cures Act violation would constitute an "independently wrongful" act sufficient to support a claim for intentional interference with prospective economic advantage under California law, even though the Cures Act lacks a private right

of action).

PointClickCare's only contrary citation is to a single District of Maryland case. *See* Opening Br. at 59 (citing *Waypoint Mgmt. Consulting, LLC v. Krone*, No. 19-cv-2988-ELH, 2022 WL 2528465, at *61 (D. Md. July 6, 2022)). Aside from being a federal district court case—not a Maryland state case—PointClickCare quotes the case out of context. All the court in that case stated was: "I am unaware of any case law that suggests that [the plaintiff] may predicate a State law claim for unfair competition on a purported violation of [a certain regulation]." *Waypoint Mgmt. Consulting*, 2022 WL 2528465, at *61. While the court did note that the regulation in question lacked a private right of action, it also noted that the duties imposed by the regulation *did not fall on the defendant*. *Id.*

We do not find that highly fact-specific, federal case particularly helpful in predicting how the Supreme Court of Maryland would decide this matter. Instead, for the reasons discussed, we think the Supreme Court of Maryland would permit a plaintiff to rely on an information-blocking violation of the Cures Act to support a claim of unfair competition.

2.

That leaves the matter of preemption. PointClickCare halfheartedly argues that Real Time's unfair-competition claim is preempted by federal law because the claim would "interfere with" federal law. Opening Br. at 61. Amici flesh out this argument, contending that in this highly regulated space, actors need a "standardized and common understanding of what conduct" violates the Cures Act—which they argue is best achieved by exclusive federal enforcement. Amicus Br. at 18.

Amici raise genuine concerns about the predictability of the law for regulated entities. But because "states are separate sovereigns," "we apply the Supremacy Clause with the basic assumption that Congress did not intend to displace state law." *N. Va. Hemp & Agric., LLC v. Virginia*, 125 F.4th 472, 492 (4th Cir. 2025) (cleaned up). This presumption "is even stronger against preemption of state remedies, like tort recoveries, when no federal remedy exists." *Coll. Loan Corp.*, 396 F.3d at 597 (quoting *Abbot ex rel. Abbot v. Am. Cyanamid Co.*, 844 F.2d 1108, 1112 (4th Cir. 1988)); *see Silkwood*, 464 U.S. at 251 ("It is difficult to believe that Congress would, without comment, remove all means of judicial recourse for those injured by illegal conduct.").

Preemption can take three basic forms: express preemption, where "Congress clearly expresses an intention for a federal law to preempt state law"; field preemption, where "Congress expresses an intent to preempt state regulation in a certain area by comprehensively regulating that area," "reflect[ing] an intent to displace state law altogether"; and conflict preemption, which occurs where either "compliance with both federal and state regulations is impossible" (direct conflict preemption) or "a state law stands as an obstacle to the accomplishment and execution of the full purposes of the federal law" (obstacle preemption). *N. Va. Hemp & Agric.*, 125 F.4th at 492–93. "A state law may pose an obstacle to federal purposes by interfering with the accomplishment of Congress's actual objectives, or by interfering with the *methods* that Congress selected for meeting those legislative goals." *Coll. Loan Corp.*, 396 F.3d at 596.

PointClickCare and Amici rely only on the second type of conflict preemption: obstacle preemption. *See* Opening Br. at 61 (arguing that allowing Real Time's unfair-

competition claim to proceed would "interfere with Congress's . . . scheme"); Amicus Br. at 15 ("[A]llowing such claims would frustrate the federal enforcement scheme Congress *did* provide."). "But a court should not find conflict preemption unless preemption was 'the clear and manifest purpose of Congress.'" *N. Va. Hemp & Agric.*, 125 F.4th at 493 (quoting *Arizona v. United States*, 567 U.S. 387, 400 (2012)). We see no such indication here. To the contrary, the Cures Act plainly contemplates that the states will regulate in this area, as it notes that information blocking can include "practices that restrict authorized access, exchange, or use *under applicable State* or Federal law." 42 U.S.C. § 300jj-52(a)(2)(A) (emphasis added).

Certainly, Congress provided a federal mechanism for resolving Cures Act violations: "[t]he inspector general of the Department of Health and Human Services . . . may investigate any claim that" an entity engaged in information blocking, and where the inspector general finds such information blocking has occurred, the Secretary of Health and Human Services must order a civil monetary penalty of up to $1,000,000 per violation. *Id.* § 300jj-52(b).

But the mere fact that Congress provided a federal executive avenue for resolving instances of information blocking is insufficient to conclusively show that Congress intended to preempt any state-law judicial cause of action based on behavior that would qualify as information blocking under the Cures Act. As we have previously held, "the fact that only the Secretary is authorized to enforce" a federal statute does not "compel the conclusion that [a plaintiff]'s pursuit of its state law claims, relying in part on violations of the [statute] or its regulations, will obstruct the federal scheme." *Coll. Loan Corp.*, 396

F.3d at 598; *see also Guthrie*, 79 F.4th at 341 ("[W]e see no reason why the mere fact that state law claims provide broader remedies than federal law means the state claims are preempted.").

And here, such an interpretation would mean that Congress recognized that states might *define* information blocking—"practices that restrict authorized access, exchange, or use under applicable State . . . law"—but, in the same breath (yet without actually explicitly saying so), forbid states from *acting on* instances of information blocking. 42 U.S.C. § 300jj-52(a)(2)(A). Neither PointClickCare nor Amici provide any explanation for how we could reach such a counterintuitive result.

We therefore conclude that Real Time may rest a Maryland unfair-competition claim in part on a violation of the Cures Act's prohibition on information blocking. So we turn to whether Real Time is likely to succeed on the merits of its assertion that there *is* such a violation here.

C.

The Cures Act describes itself as "An Act [t]o accelerate the discovery, development, and delivery of 21st century cures." 21st Century Cures Act, 130 Stat. at 1033. It includes provisions related to a wide variety of health-related issues, including the opioid epidemic, drug development, vaccine access, and more. *Id.* § 1, 130 Stat. at 1033–35. Notably for our purposes, it seeks to prevent companies from engaging in "information blocking" of electronic health information. *Id.* § 4004, 130 Stat. at 1176 (codified as amended at 42 U.S.C. § 300jj-52).

As relevant here, the Cures Act defines "information blocking" as a practice that,

"except as required by law or specified by the Secretary [of Health and Human Services] pursuant to rulemaking . . . , is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information," and which "a health information technology developer, exchange, or network . . . knows, or should know, . . . is likely to" have these effects. 42 U.S.C. § 300jj-52(a)(1)(A)–(B)(i); *see id.* § 201(c). As the Department of Health and Human Services put the point in its related rulemaking, these statutory provisions "are designed to advance interoperability" and "support the access, exchange, and use of electronic health information." 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25642, 25643 (May 1, 2020).

PointClickCare concedes that using indecipherable CAPTCHAs and locking users out facially constitutes information blocking under the Cures Act, absent an applicable exception. Oral Arg. at 3:40–3:48, https://www.ca4.uscourts.gov/OAarchive/mp3/24-1773-20250128.mp3. But it contends that its activities do *not* constitute information blocking, by definition, because they are activities that "[t]he Secretary, through rulemaking," has "identif[ied] [as] reasonable and necessary." 42 U.S.C. § 300jj-52(a)(3). It points to three exceptions identified in the regulations: the manner exception, the health-IT-performance exception, and the security exception.

Before turning to those exceptions, we pause to discuss the question of burden. PointClickCare took the position below that Real Time had to affirmatively demonstrate that the exceptions did *not* apply. *See* J.A. 965 (PointClickCare arguing that, at the preliminary-injunction stage, Real Time carries the burden not only of establishing its own

case, but also "of disproving [PointClickCare's] case"; that is, Real Time "bear[s] the burden in eliminating our defenses"). The district court disagreed. *See* J.A. 885 (court noting that once Real Time had shown information blocking, "it's up to the defense to show that one of these exceptions applies," which was "the defense['s] burden").

On appeal, PointClickCare has repeatedly insisted in a general way that the district court "misapplied the burden of proof." Opening Br. at 4. Yet it failed to explain in its opening brief why the district court was wrong that the exceptions set forth in the regulations are defenses to the applicability of the information-blocking statute on which it would bear the burden of proof at trial.

In any event, we think the district court was correct. Assigning the burden in this way—where Real Time must show that PointClickCare engaged in facial information blocking, and then the burden shifts to PointClickCare to show that its actions were *not* information blocking because a regulatory exception applies—aligns with the purpose of the Cures Act's prohibition on information blocking by putting the onus on the party engaging in such blocking to demonstrate that it is doing so for good reason. And as noted above, it is well established that "the burdens at the preliminary injunction stage track the burdens at trial." *Gonzales*, 546 U.S. at 429. The district court thus appropriately held PointClickCare to the burden of establishing that one of the exceptions applied. We do the same and agree with the district court that PointClickCare has not satisfied that burden based on the present record.

1.

We begin with the manner exception. That exception provides that "[a]n actor must

fulfill a request for electronic health information *in any manner requested*, unless the actor is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the request in the manner requested." 45 C.F.R. § 171.301(a)(1) (emphasis added). "If an actor does not fulfill a request for electronic health information in any manner requested because it" successfully invokes § 171.301(a)(1), "the actor must fulfill the request in an alternative manner," as defined in § 171.301(b)(1). *Id.* § 171.301(b).

Notably, an actor must fulfill a request for *all* electronic health information requested, as defined by 45 C.F.R. § 171.102. Today's manner exception refers only to the *manner* of delivery, not the *content* to be delivered. And this was a deliberate choice. The exception was originally labeled the "[*c*]*ontent and* manner exception" because it originally included a content condition. 21st Century Cures Act, 85 Fed. Reg. at 25959 (emphasis added).

Specifically, when the Department of Health and Human Services enacted the regulations creating the manner exception in May 2020, it explicitly limited the data that an actor must provide for the first two years to "the electronic health information identified by the data elements represented in the USCDI standard adopted in § 170.213." *Id.* (codified as amended at 45 C.F.R. § 171.301). It later extended that deadline for another five months, until October 2022, due to the COVID pandemic. Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency, 85 Fed. Reg. 70064, 70085 (Nov. 4, 2020) (codified as amended at 45 C.F.R. § 171.301). These delays were intended to ensure that actors would have time to ramp up compliance with the manner exception. 21st

Century Cures Act, 85 Fed. Reg. at 25795.

However, in 2024, the Department modified the regulation to remove the content provision and to change the exception's label to "manner exception" to reflect "that the 'content' condition . . . has been moot since October 6, 2022." Health Data, Technology, and Interoperability: Certification Program Updates, Algorithm Transparency, and Information Sharing, 89 Fed. Reg. 1192, 1373 (Jan. 9, 2024); *see id.* at 1437; *cf. id.* at 1199 ("On and after October 6, 2022, the scope of [electronic health information] for purposes of the 'information blocking' definition (§ 171.103) is [electronic health information] as defined in § 171.102."). The Department was not persuaded against this change by commenters concerned about situations where they might only be able to fulfill a request for *some* of the electronic health information requested. Instead, the Department suggested that, "[i]n such instances, an actor may want to consider whether another exception is applicable to any other requested [electronic health information]." *Id.* at 1373. The Department's explanation for the rulemaking thus implies that applicable exceptions to requests for electronic health information should be analyzed separately for each category of electronic health information requested. *Id.*

In the fall of 2023, Real Time made a two-part "request for electronic health information." 45 C.F.R. § 171.301(a)(1). PointClickCare has not contended that any of the sought-after data falls outside the definition of "electronic health information" set forth in 45 C.F.R. § 171.102, so it needed to provide Real Time with *both* segments of this data unless an exception applied. The first part, related to roughly 70% of the data Real Time requires, pertained to the proposed data export. That data-export solution was the focus of

the district court's written opinion finding that the manner exception did not apply. *Real Time*, 2024 WL 3569493, at *10.

Yet PointClickCare does not grapple with that conclusion *at all* in its opening brief.[12] And because PointClickCare has undisputedly blocked Real Time's access to this requested data, Real Time is likely to succeed on the merits of its claim on this basis alone (unless a different exception applies).

For completeness, we nevertheless address the second part of Real Time's request. For the other 30% or so of data that Real Time requires, it requested access through the Marketplace API. PointClickCare does not claim any technical difficulty with granting such access. Rather, it contends that the parties "cannot reach agreeable terms." Opening Br. at 34 (quoting 45 C.F.R. § 171.301(a)(1)).

PointClickCare apparently believes that "cannot reach agreeable terms" has the same meaning as "have not reached agreeable terms," even where that lack of agreement is due to the information-blocking party's unexplained unwillingness to agree. *See* J.A.

[12] Even if PointClickCare had challenged the district court's conclusion on this point, we see no error. As we conclude below, PointClickCare must show some good-faith efforts to reach agreeable terms before claiming that it "cannot" do so. But PointClickCare has provided no evidence whatsoever that the data export was technically impossible or not to its liking for other reasons. To the contrary, it could not provide a reason the conversations around the matter stopped when repeatedly asked about it by the district court at the hearing. Nor did it give any reason at oral argument before this Court why the data-export proposal was not agreeable to it under § 171.301(a), despite being pressed on the point multiple times. Oral Arg. at 4:35–5:30, 13:20–13:44 (making only an argument under the *alternative-manner* section of the regulation, § 171.301(b), even though that provision is irrelevant if PointClickCare cannot first satisfy § 171.301(a)); *see id.* at 9:15–10:39. By contrast, Real Time introduced significant testimony supporting that a data export would be a relatively simple solution for which it would be willing to pay—both to build in the first place and for ongoing access.

939, 945 (PointClickCare arguing before the district court that the fact that the parties *had not* reached an agreement, alone, was enough to show the parties "cannot reach agreeable terms" for purposes of the manner exception); Oral Arg. at 12:31–12:41 (PointClickCare arguing that the district court erred because of its "legally inaccurate premise that being unwilling [to come to an agreement] doesn't get you into the manner exception").

We disagree. For the phrase "cannot reach agreeable terms" to carry any weight, it must imply at least some reasonable efforts and articulable reasons why the parties *cannot* come to an agreement. *See* J.A. 951 (district court pointing out that the regulation does not say "have not reached" agreeable terms, it says "*cannot*," implying some level of good faith and the need to articulate *some* reason for the impasse (emphasis added)); *cf.* 21st Century Cures Act, 85 Fed. Reg. at 25877 ("These provisions will allow actors to first attempt to negotiate agreements in any manner requested with whatever terms the actor chooses and at the 'market' rate—which supports innovation and competition.").

That's because the only reason a defendant would *ever* invoke the manner exception—save a technical barrier—would be if the defendant did not *want* to provide the information in the manner requested. And why would a defendant go to the trouble of trying to demonstrate that it was "technically unable to fulfill the request" if it could simply assert that it had no *desire* to fulfill the request?

Notably, it is quite difficult to show that a party is "technically unable" to fulfill a request. "This standard sets a very high bar, and would not be met if the actor is technically able to fulfill the request, but chooses not to fulfill the request in the manner requested due to cost, burden, or similar justifications." 21st Century Cures Act, 85 Fed. Reg. at 25877.

Rather, cost concerns can be resolved through "charg[ing]" higher "fee[s]," and a truly burdensome request might be subject instead to the separate "[i]nfeasibility [e]xception." *Id.* (citing 45 C.F.R. § 171.204). If PointClickCare's interpretation is correct, however, the actor could skirt the "very high bar" of the "technically unable" prong merely by claiming, with no need to support its assertion, that it "cannot reach agreeable terms with the requestor."

In sum, if PointClickCare's interpretation is correct—that it can just refuse a request for electronic health information, and through that refusal bypass § 171.301(a)—that provision has essentially no meaning.

Consider also the role of 45 C.F.R. § 171.301(b). Under that provision, "[i]f an actor does not fulfill a request for electronic health information in any manner requested because" it can satisfy § 171.301(a)(1)—such as by showing that the parties "cannot reach agreeable terms"—then it "must fulfill the request in an alternative manner," as set forth in a preferred order in the regulation. 45 C.F.R. § 171.301(b). PointClickCare contends that it satisfies the first-preferred alternative manner for the *entirety* of Real Time's request by offering its USCDI system, even though that data only constitutes 30% of Real Time's requested data. *Id.* § 171.301(b)(1)(i); *see* J.A. 943 ("THE COURT: So if USCDI is only 30 percent of the record that the authorized user needs to perform its role for its customer, they are just out of luck? [POINTCLICKCARE'S COUNSEL]: At its most basic, that's what the regulations require us to do if we fail to reach an agreement, so, yes, Your Honor.").

We have already rejected PointClickCare's interpretation on this point, concluding

instead that PointClickCare must satisfy the manner exception *separately* for each category of requested data. Assuming for the sake of argument that PointClickCare is correct that its USCDI system would fully qualify as an alternative manner for *all* of Real Time's requested data, however, such an interpretation would further undermine PointClickCare's highly limited view of "cannot reach agreeable terms." As noted, the Department initially specifically allowed actors to fulfill requests by providing only USCDI-mandated information for a limited period after the regulation's enactment. It would be passing strange if, after those deadlines had come and gone, an actor could invoke its offer of access to the USCDI system as full compliance with the manner exception merely by claiming that the parties could not reach agreeable terms.

The district court agreed with this interpretation of the rule. Applying that interpretation to the facts here, the court found that "the record does not suggest that [PointClickCare] can find no 'agreeable terms' for alternatives. Indeed, the parties were well on their way to a mutually agreeable alternative whereby Real Time would pay [PointClickCare] to export the data not otherwise available through [the Marketplace] API. [PointClickCare] inexplicably chose to end those discussions and so it now cannot reap the benefit of this exception. In a nutshell, [PointClickCare] appears more unwilling than unable to reach a mutually agreeable solution. [PointClickCare] cannot take cover under the manner exception." *Real Time*, 2024 WL 3569493, at *10 (citations omitted).

PointClickCare does not argue that the district court committed clear error in its

factual findings on this point, and we see none.[13] The present record shows that the parties began negotiations around Marketplace API access, including those related to the appropriate fee and to the terms of the agreement. Technical employees began building out the required structure. PointClickCare concedes that it has modified the standard terms of the agreement before entering contracts with other companies. And it asked Real Time to send proposed redlines to the agreement. Yet it prematurely cut off talks without responding to Real Time's proposed redlines or proposed fee structure. The parties had not yet reached an impasse; PointClickCare presented its standard terms, Real Time countered, and PointClickCare simply "went silent," at which point "the negotiations ceased without further explanation." *Id.* at *3. We agree with the district court that that is not enough to support PointClickCare's burden to show that the parties "cannot reach agreeable terms."

To be sure, is it not our role to flyspeck negotiations between two sophisticated parties to determine whether they have exhausted every possible avenue of agreement and force them to return to the negotiating table again and again. But the purpose of the information-blocking provision of the Cures Act is to encourage the "access, exchange, or use of electronic health information," including to ensure that "complete information sets"

[13] During the hearing below, the court asked PointClickCare what made it "unable to continue the conversations," asking, "is there any testimony that I missed . . . [to the effect that] what they are asking for is the sun and the moon, and we can't do it? We can't do it technically, it's too expensive? We told them you have to pay us X dollars, and they said no? See, I didn't hear any of that. What I heard was there was a back-and-forth, and then there wasn't." J.A. 939. PointClickCare responded that the parties were simply "not able to reach an agreement yet. Maybe we will in the future, so it's a possibility. But to date, we cannot reach an agreement." *Id.* We note that if there remains the "possibility" of agreement between the parties, it is simply not true that the parties definitively "*cannot* reach agreeable terms." If the door remains open, it remains open.

are "export[ed]" and that innovative technologies, particularly in "care delivery," are not "impede[d]." 42 U.S.C. § 300jj-52(a)(1)(A), (2)(C)(i)–(ii). And the Department of Health and Human Services has informed us that "each exception is intended to be tailored, through appropriate conditions, so that it is limited to the reasonable and necessary activities that it is designed to exempt." 21st Century Cures Act, 85 Fed. Reg. at 25649.

Further, the Department chose the approach it did in the manner exception "because [it] believe[s] actors should, first and foremost, attempt to fulfill requests to access, exchange, or use [electronic health information] in the manner requested" in order to "help ensure that [electronic health information] is made available where and when it is needed." *Id.* at 25877. It simply cannot be the case that the holder of electronic health information can get around these statutory and regulatory goals merely by claiming an inability to reach agreeable terms without any evidence of genuine efforts being made to do so.

2.

PointClickCare also invokes the health-IT-performance and security exceptions. As relevant here, the health-IT-performance exception provides that "[a]n actor may take action against a third-party application that is negatively impacting the health IT's performance, provided that the practice is . . . [i]mplemented in a consistent and non-discriminatory manner." 45 C.F.R. § 171.205(b)(2). Similarly, as relevant here, the security exception applies where "[a]n actor's practice that is likely to interfere with the access, exchange, or use of electronic health information in order to protect the security of electronic health information" is "tailored to the specific security risk being addressed" and "implemented in a consistent and non-discriminatory manner." *Id.* § 171.203(b)–(c).

The district court concluded that PointClickCare's bot-prevention policy was not "implemented in a consistent and non-discriminatory manner," precluding PointClickCare's reliance on either of these exceptions. *Real Time*, 2024 WL 3569493, at *8; *see id.* at *9–10. Yet again, PointClickCare fails to counter this conclusion in its opening brief.

In any event, we agree with the district court. It is true that users other than Real Time's were watch-listed. However, there is no evidence—beyond the say-so of Fourati, whose explanations the district court found lacking—as to whether those non-Real-Time users were in fact presented with indecipherable CAPTCHAs or blocked. Even assuming they were, Fourati testified that PointClickCare did not know which users belonged to Real Time (unless the username explicitly referred to Real Time) until Real Time provided a list of users in May 2024. So, even if other users' bots were caught up in the same net as Real Time's, that does not mean the net was not *aimed* at Real Time. To the contrary, the timing of the introduction, escalation, de-escalation, and re-escalation of the CAPTCHAs and blocking policy—corresponding with PointClickCare's entrance into the field as a competitor and various discussions with Real Time, including receiving significant sensitive information from Real Time under the NDA—is highly suggestive that these actions were targeted at Real Time. *Id.* at *10–11.

The sporadic nature of PointClickCare's challenged actions also demonstrates that they have not been exercised consistently. First, PointClickCare has not been consistent in taking action related to bot activity at all. There is no evidence that PointClickCare has ever sued a customer to enforce the anti-bot provision of its contracts. Real Time used bots

over many years and never heard a peep from PointClickCare that it objected to their use, even when Real Time specifically contacted PointClickCare to let it know that it was reducing its data pulls in light of the initial round of (solvable) CAPTCHAs.

Second, PointClickCare has not implemented the unsolvable CAPTCHAs in a consistent manner. Real Time introduced testimony that it saw very few unsolvable CAPTCHAs from roughly February to May 2024. This assertion is supported by PointClickCare's own exhibit, which, as the district court noted, showed a user operating at what was (according to PointClickCare's criteria) clearly a bot level of resource use from November 2023 to May 2024 without being watch-listed. PointClickCare's explanation on this point was that it was "very reticent . . . to put somebody on a watch list and/or block them." J.A. 923. But such "reticence" does not provide a clear metric for consistency. Nor is it supported by the record, where Real Time introduced uncontradicted testimony that it was repeatedly swiftly (i.e., within days or weeks) locked out of access to accounts for *hundreds* of its skilled-nursing-facility customers that used PointClickCare's system. *Cf.* Opening Br. at 50 (PointClickCare asserting that, "when [it] detects bot activity, it must act to block the threat to its system").

We also agree with the district court's conclusion that PointClickCare's reliance on these exceptions fails for other reasons. As relevant here, the health-IT-performance exception only applies where "a third-party application . . . is negatively impacting the health IT's performance." 45 C.F.R. § 171.205(b). But, other than two charts from April 2023, PointClickCare provided only extremely broad testimony that it experiences slowdowns caused by bot activity. *See Real Time*, 2024 WL 3569493, at *5–6. As for those

two charts, they are from well before any of the challenged actions in this case. And they show only that a user—one that, according to Fourati, a customer said belonged to Real Time—was using significant resources around the time that PointClickCare received a customer complaint regarding system performance. That extremely limited and tenuous evidence is not enough to demonstrate that Real Time's bot usage is an ongoing threat to PointClickCare's system performance. This is particularly so given that Real Time is a small player in the grand scheme of PointClickCare's work: Real Time works with only 1,400 of PointClickCare's 27,000 facilities (or five percent), and PointClickCare itself pushes out 1.2 million medication administrations per day by automated process. *See* J.A. 957 (district court raising doubts about Fourati's testimony as "vague and nonspecific and unsupported" because he also testified to PointClickCare "push[ing] out 1.2 million medication administrations a day . . . by automated activity" with no issue); *Real Time*, 2024 WL 3569493, at *6, *8.

PointClickCare also did not introduce any evidence to indicate that it had ongoing service issues for the decade during which Real Time was using bots to access its system; that its performance improved when Real Time reduced its number of data pulls by half (and then by half again); or that its system's performance improved when it introduced indecipherable CAPTCHAs and locked Real Time's users out. Further underlining the tenuousness of PointClickCare's alleged performance concerns is one of its own declarations: an executive at a senior-care provider stated that his company relied on PointClickCare's systems and explained that while his company had "*generally never had a problem* accessing any of PointClickCare's services," there had been "a *handful* of

instances" where employees complained about the systems "working at a *slower rate* than usual," which PointClickCare "*informed* [*them*] . . . *may* be caused when vendors engage in an excessive use of the system which *may* cause system timeouts." J.A. 330 (emphasis added).

Simply put, while PointClickCare could eventually come forward with evidence that Real Time's bot usage "negatively impact[s] [its] performance," 45 C.F.R. § 171.205(b), it has to date failed to carry its burden to establish that basic fact.

As for the security exception, an act that would otherwise constitute information blocking only falls under that exception if it is "tailored to the specific security risk being addressed." *Id.* § 171.203(b). But PointClickCare has failed to articulate a specific security risk posed by Real Time's bot access, instead gesturing very broadly to the potential malicious use of bots. *Real Time*, 2024 WL 3569493, at *9–10.

In fact, instead of providing evidence, PointClickCare baldly argues that the notion "that third-party bots are a systemic security risk to its platform" is "an obvious point that should not require documentation." Opening Br. at 4. But *any* access to *any* electronic system poses security risks, so that kind of vague assertion is not enough to evade the statutory ban on information blocking. And there is no evidence that Real Time's use of bots in PointClickCare's system has ever led to any security breach; in fact, there is no evidence of a security breach experienced by Real Time at all. Moreover, Real Time possesses the highest level of security certification. There is simply no evidence that Real Time's use of bots poses a genuine security concern for PointClickCare. *See Real Time*, 2024 WL 3569493, at *3 n.2 ("Real Time . . . seems to pose no identifiable security threat

to [PointClickCare].").

Further, even if PointClickCare is truly concerned about users downloading vast quantities of data from its systems, it did not express this concern for years before it started seeking to become a competitor. Human users, to which it does not object, can also download such vast quantities of data. *See id.* (finding that Real Time's "automated software poses no greater risk of a security breach than that associated with human users"). And more tailored means are available—simply obtaining usernames from Real Time (or from its customer) would allow PointClickCare to ensure that a user it sees downloading large quantities of data is an authorized one, and performing random quality checks such as contacting Real Time or its customer when it sees a user downloading large quantities of data would enable it to ensure the authorized user's IP address was not being "spoofed" by a nefarious actor. *See* J.A. 489 (noting that spoofing is when a malicious actor makes "their IP address . . . look like somebody else's IP address").

In sum, we agree with the district court that none of the exceptions that PointClickCare invokes apply. Real Time is likely to succeed on the merits of its claim that PointClickCare's use of indecipherable CAPTCHAs and blocking of user accounts constitutes information blocking under the Cures Act.

D.

Finally, PointClickCare argues that even if we conclude that Real Time can rely on the Cures Act in part to establish an unfair-competition claim, and even if its actions violate the Cures Act, Real Time is nevertheless unlikely to succeed on the merits of its unfair-competition claim because (1) it cannot satisfy the other elements of that claim and (2) such

an interpretation of the Cures Act would pose an avoidable constitutional concern. We disagree.

PointClickCare argues that even if its actions violate the Cures Act, Real Time "cannot show that PointClickCare engaged in any sort of fraud or deception," which "is fatal to its unfair-competition claim." Opening Br. at 65. That is wrong. As noted, the law of unfair competition includes "damaging or jeopardizing another's business by fraud, deceit, trickery *or unfair methods of any sort*." *Balt. Bedding Corp.*, 34 A.2d at 342 (emphasis added); *accord Mascaro v. Snelling & Snelling of Balt., Inc.*, 243 A.2d 1, 10 (Md. 1968) ("As the law developed, proof of fraudulent deception was no longer essential for relief, and this is the Maryland rule."); *Paccar*, 905 F. Supp. 2d at 690–92 (reviewing relevant case law). Illegal actions directed at a competitor are unfair. *Cf. Command Tech.*, 2015 WL 6470277, at *8. And at bottom, we agree with the district court that the present record strongly supports an inference that PointClickCare sought to leverage its control over its EHR system to harm Real Time's business, and that its cited reasons for its actions (security and system performance) were a cover for its true motivations (hurting a competitor). *See Real Time*, 2024 WL 3569493, at *11.

PointClickCare also argues that "[t]he district court's misinterpretation of the Cures Act raises grave constitutional questions" under the Takings Clause and urges this Court to employ the constitutional-avoidance canon to interpret the Act differently. Opening Br. at 53. Yet it does not even cite, much less explain how the facts of this case would satisfy, the factors relevant to a takings claim of this type. *See Blackburn v. Dare County*, 58 F.4th 807, 810–11 & n.3 (4th Cir. 2023). Thus, we decline to address this argument.

We affirm the district court's conclusion that Real Time is likely to succeed on the merits of its unfair-competition claim. We therefore do not reach the tortious-interference claim.

IV.

Because we agree with the district court that Real Time has demonstrated a sufficient likelihood of success on the merits of at least one of its claims, we turn to the remaining preliminary-injunction factors. We agree with the district court that Real Time has satisfied them.

A.

First is the question of irreparable harm. The district court correctly noted that irreparable harm can include "actual and imminent" "loss of good will or erosion of [a company's] customer base." *Real Time*, 2024 WL 3569493, at *12; *see Multi-Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 552 (4th Cir. 1994) (describing the "permanent loss of customers to a competitor or the loss of goodwill" as a form of irreparable injury), *abrogated in part on other grounds by Winter*, 555 U.S. 7; *Air Evac EMS, Inc. v. McVey*, 37 F.4th 89, 103 (4th Cir. 2022) (noting impending likely "loss of customers and employees" as irreparable harm).

PointClickCare's actions threaten exactly that: every time Real Time must reach out to a customer to ask them to reset an account, it wastes the customer's time and looks incompetent to the customer. And every time Real Time's access to the records for a given nursing home is disrupted, that is "a 100% business interruption" with that facility. *Real Time*, 2024 WL 3569493, at *12. The disruption of Real Time's ability to do its work with

hundreds of facilities at a time—700 and 600 in November 2023 and May 2024, respectively, out of its 1,700 customer facilities—puts it at immediate risk of breach of its contracts with its customers and "presents a real and imminent threat to [its] continued ability to do business." *Id.*; *see* J.A. 428 (Dr. Rifkin conceding that Real Time has not yet received notice from a customer that the customer was terminating a contract related to the loss of service, but attributing this to the fact that Real Time "ha[s] been able to provide service because [PointClickCare] backed off on the CAPTCHAs" in light of the litigation); J.A. 438 (Dr. Rifkin testifying that Real Time "will be out of business within weeks if [it is] shut off from the data"); J.A. 611–12 (Buono agreeing with Dr. Rifkin's assessment and explaining that most of Real Time's revenue comes from larger contracts, like that with CRISP, and that "given PointClickCare's market share," if PointClickCare cuts off Real Time's access, Real Time would not be able to "perform the analytics" it is required to perform under those contracts).

While PointClickCare argues that Real Time could access the data in other ways, the record does not support any immediately viable alternatives that would avoid these irreparable harms. The Marketplace or USCDI systems provide only about 30% of the necessary data and involve a contract that, without modifications, would arguably place Real Time in immediate breach. Hiring 450 humans to replace the bots would risk breach of Real Time's contracts with its customers during the significant time it would take to hire and train these individuals, and would carry a substantial risk of financial ruin once they were hired because the cost of staffing would exceed Real Time's revenues from its customers. The only truly viable alternatives—a modified data relay or data export

combined with the Marketplace—are ones that PointClickCare has refused to allow Real Time to pursue.

B.

Next is the matter of the balance of the equities. The district court concluded that "were [PointClickCare] permitted to use unsolvable CAPTCHAs in the future, Real Time would face unpredictable, unplanned widespread business outages akin to that which it has withstood before. [PointClickCare], on the other hand, has given the Court no reason to believe that eliminating the use of such unsolvable CAPTCHAs would visit any harm to it. The narrow relief requested leaves intact nearly all of [PointClickCare]'s existing security protocol, including the use of solvable CAPTCHAs, and enjoins solely the use of unsolvable CAPTCHAs which do not rationally relate to the provision of security in any event." *Real Time*, 2024 WL 3569493, at *12.

We agree. Solvable CAPTCHAs will still stop some bots from accessing PointClickCare's systems, and as discussed, it has presented no more than broad-strokes evidence that bots pose a risk to its systems anyway. On the flip side, allowing it to use unsolvable CAPTCHAs will rapidly place Real Time in an untenable position, as described above. Further, as the district court noted, even if Real Time pursued the supposed "solution" of hiring 450 human users, it is not clear this would be better for either party. Rather, it "stands to reason that automated software used by a company with the highest security certification remains more secure than if the same company had to employ 450 individuals to perform the same task." *Id.* at *9 n.5. It also seems highly likely that utilizing 450 human staff members to download the needed data would introduce more errors into

that data, risking Real Time's ability to perform its role quickly and accurately. Balancing the potential harms to Real Time from not having an injunction against those to PointClickCare from having one, we readily agree with the district court that the equities favor Real Time's position.

C.

Finally, we must consider the public interest. The district court focused on the benefits provided by Real Time's services. *Id.* at *12. PointClickCare made clear below that it does not dispute that Real Time provides meaningful services, the continuation of which is in the public interest. And the record supports that Real Time's inability to perform its work threatens real harm to patients, including the very real potential for increased nursing-home deaths. One witness who works closely with Maryland's CRISP program testified that, if Real Time stopped being able to provide its services to CRISP, "for want of another substitute that would immediately step in and do that, people are at risk of death"—and that such an immediate substitute was unlikely because the state government's request-for-proposal process moves slowly, so CRISP would not be able to "pivot quickly to find another . . . service supplier." J.A. 567, 570. He also explained that the patients at risk are "not only the oldest and most vulnerable Marylanders, they are also, by definition, the poorest" and "don't have the options to be in a high-level assisted living community or to have . . . around-the-clock home care." J.A. 571.

Of course, PointClickCare also provides valuable services, so a genuine threat to those services would be of grave concern as well. But we agree with the district court that the evidence suggests that Real Time's use of bots does not pose a risk to PointClickCare's

ability to do its business—and certainly not such a grave risk so as to outweigh the threat that PointClickCare's use of indecipherable CAPTCHAs and user blocking poses to Real Time's ability to provide *its* valuable services. In fact, as the district court found, it appears likely that such a threat to Real Time's ability to provide its services was precisely the point of PointClickCare's enjoined actions. *Real Time*, 2024 WL 3569493, at *11. The public interest does not weigh in favor of such anticompetitive and harmful behavior.

V.

For the foregoing reasons, we affirm the district court's order granting a preliminary injunction to Real Time.

AFFIRMED